

CIPT1

Implementing Cisco Unified Communications IP Telephony Part 1

Volume 2

Version 6.0

Student Guide

Editing, Production, and Web Services: 02-15-08



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 563-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, Gigabit Drive, 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)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Volume 2

<u>Single-Site Off-Net Calling</u>	4-1
Overview	4-1
Module Objectives	4-1
<u>Implementing MGCP Gateways in Cisco Unified Communications Manager</u>	4-3
Overview	4-3
Objectives	4-3
Cisco Unified Communications Manager and MGCP Gateways	4-4
Endpoint Identifiers	4-5
MGCP and SCCP Interaction	4-6
MGCP Gateway Support in Cisco Unified Communications Manager and Cisco IOS Gateways	4-7
Cisco Unified Communications Manager Configuration Server	4-11
PRI Backhaul	4-12
MGCP Gateway Configuration in Cisco Unified Communications Manager	4-13
Step 1: Add an MGCP Gateway	4-14
Step 2: MGCP Gateway Configuration	4-16
Steps 3 and 4: Add MGCP Endpoints by Selecting Modules and VICs	4-17
Step 5: Configure the MGCP Endpoint	4-19
Cisco IOS Gateway MGCP Configuration	4-21
Configuring Cisco IOS Gateway for MGCP Using a Configuration Server	4-23
Configuring Cisco IOS Gateway for MGCP – Example	4-25
Summary	4-27
<u>Configuring Cisco Unified Communications Manager Call Routing Components</u>	4-29
Overview	4-29
Objectives	4-29
Endpoint Addressing	4-30
Endpoint Dialing	4-31
Endpoint Dialing Example	4-32
Uniform On-Net Dial Plan Example	4-33
Cisco Unified Communications Manager Call Routing	4-35
Call Routing Types Example	4-36
Call Routing Table Entries (Call Routing Targets)	4-37
Sources of Call Routing Requests (Entities Requiring Call Routing Table Lookup)	4-38
Route Patterns: Commonly Used Wildcards	4-39
Route Pattern Examples	4-40
Cisco Unified Communications Manager Call Routing Logic	4-41
Digit-by-Digit Analysis	4-42
Digit Collection Example	4-43
Closest Match Routing Example	4-44
Interdigit Timeout Example	4-45
Cisco Unified Communications Manager Digit Analysis	4-46
User Input on SCCP Phones	4-47
User Input on SIP Phones	4-48
User Input on Type A SIP Phones – No SIP Dial Rules Configured on the Phone	4-49
User Input on Type A SIP Phones – SIP Dial Rules Configured on the Phone	4-50
User Input on Type B SIP Phones – No SIP Dial Rules Configured on the Phone	4-51
User Input on Type B SIP Phones – SIP Dial Rules Configured on the Phone	4-52
Dial Rules and KPMI Interworking	4-53
Gateway Overlap Sending and Receiving	4-54
Cisco Unified Communications Manager Path Selection	4-55
Path Selection Example	4-56
Path Selection Configuration Elements in Cisco Unified Communications Manager	4-57
Cisco Unified Communications Manager Path Selection Configuration	4-58
Route Group Configuration	4-59
Route Group Configuration	4-60
Route List Configuration	4-61
Route List Configuration Example	4-62

Digit Manipulation Requirements with Path Selection	4-63
Special Call Routing Features	4-64
Route Filters	4-65
The ! Wildcard	4-68
Urgent Priority	4-69
Blocked Patterns	4-70
Call Classification	4-71
Summary	4-72
References	4-72
Implementing Cisco Unified Communications Manager Digit Manipulation	4-73
Overview	4-73
Objectives	4-74
Essentials of Cisco Unified Communications Manager Digit Manipulation	4-75
Digit Manipulation Requirements	4-76
Cisco Unified Communications Manager Digit Manipulation Flow	4-77
Digit Manipulation Flow Example (Incoming Call from PSTN)	4-78
Cisco Unified Communications Manager Digit Manipulation Configuration Elements	4-79
Cisco Unified Communications Manager External Phone Number Mask	4-80
Configuring External Phone Number Mask	4-81
External Phone Number Mask Example	4-82
Cisco Unified Communications Manager Digit Prefix and Stripping	4-83
Digit Stripping	4-84
Understanding DDIs	4-85
Using PreDot DDIs	4-86
Using Compound DDIs	4-87
Cisco Unified Communications Manager Transformation Masks	4-88
Configuring Transformation Masks	4-89
Cisco Unified Communications Manager Translation Patterns	4-90
Configuring a Translation Pattern	4-92
Translation Pattern Example	4-93
Cisco Unified Communications Manager Significant Digits	4-94
Configuring Significant Digits	4-95
Significant Digits Example	4-96
Cisco Unified Communications Manager Digit Manipulation	4-97
Calling Party Transformation Order	4-98
Called Party Transformation Order	4-99
Transformation Example	4-100
Summary	4-101
References	4-102
Implementing Calling Privileges in Cisco Unified Communications Manager	4-103
Overview	4-103
Objectives	4-103
Calling Privileges Fundamentals	4-104
Call Privileges Requirement Example	4-105
Calling Privileges Configuration Elements	4-106
Partitions and Calling Search Spaces	4-107
Partition <None> and CSS <None>	4-108
Analogy: Locks and Key Rings	4-109
Basic Partitions and CSS Example	4-111
CSS Partition Order Relevance	4-112
Partitions and CSS Example with Multiple Best Matches	4-113
Phones Have a Device CSS and Line CSS	4-114
Example with IP Phone Line CSS and Device CSS	4-115
Class of Service Sample Scenario	4-117
Configuring Partitions and Calling Search Spaces	4-119
Creating Partitions	4-120
Assigning Partitions	4-121
Creating a CSS	4-122
Assigning a CSS to an IP Phone	4-123

Time Schedules and Time Periods	4-124
Time-of-Day Routing Applications	4-125
Time Periods and Time Schedules	4-126
Example: Block International Calls During Weekends and on January 1	4-127
Time-of-Day Routing Configuration Procedure	4-128
Creating Time Periods	4-129
Creating Time Schedules	4-130
Assigning Time Schedules to Partition	4-131
Understanding CMC and FAC	4-132
CMC Call: Successful Call	4-133
CMC Call: Call Failure	4-134
FAC Call: Successful Call	4-135
FAC Call: Call Failure	4-136
Calling Privileges Applications Overview	4-137
Calling Privileges Application Examples	4-138
Implementing CoS	4-139
Implementing CoS: Traditional Approach	4-140
Traditional Approach – Example: Single Site	4-141
Traditional Approach – Example: Multiple Sites	4-142
Line Device Approach: Improves Scalability	4-143
Using a Line Device Approach	4-144
Line Device Approach – Example: Multiple Sites	4-145
Implementing 911 and Vanity Numbers	4-146
Vanity Numbers	4-147
Implementing Emergency and Vanity Numbers in Cisco Unified Communications Manager	4-148
Vanity Number Example	4-149
Implementing Time of Day-Based Carrier Selection	4-150
Time of Day-Based Carrier Selection Example	4-151
Implementing PLAR	4-152
PLAR Example	4-153
Summary	4-155
References	4-156

Implementing Call Coverage in Cisco Unified Communications Manager

4-157

Overview	4-157
Objectives	4-157
Cisco Unified Communications Manager Call Coverage Features	4-158
Cisco Unified Communications Manager Call Forwarding, Shared Lines, and Call Pickup	4-159
Shared Lines	4-160
Call Pickup/Group Call Pickup	4-161
Call Hunting Components	4-162
Call Hunting Operation	4-163
Hunt Pilots	4-164
Hunt Lists	4-166
Line Groups	4-167
Line Group Members	4-168
Call Hunt Options and Distribution Algorithms	4-169
Line Group Distribution Algorithms	4-170
Call Hunting Flow	4-171
Call Hunting Configuration	4-174
Step 1: Configuring Line Groups	4-175
Step 2: Configuring Hunt Lists	4-177
Step 3: Configuring Hunt Pilots	4-179
Directory Number Configuration	4-181
Example 1: Internal and External Forwarding (No Hunting)	4-183
Example 2: Internal and External Forwarding with Hunting	4-184
Example 3: Internal and External Forwarding with Hunting	4-185
Example 4: Internal and External Forwarding with Hunting	4-186
Example 5: Using the Maximum Hunt Timer While Hunting	4-187
Summary	4-188
References	4-188

Module Summary	4-189
References	4-190
Module Self-Check	4-191
Module Self-Check Answer Key	4-198
<i>Implementation of Media Resources, Features, and Applications</i>	5-1
Overview	5-1
Module Objectives	5-1
Implementing Media Resources	5-3
Overview	5-3
Objectives	5-3
Understanding Media Resources	5-4
Media Resources Functions	5-5
Cisco Unified Communications Manager Media Resources Support	5-7
Media Resource Signaling and Audio Streams	5-8
Voice Termination Signaling and Audio Streams	5-9
Audio Conferencing Signaling and Audio Streams	5-10
Transcoder Signaling and Audio Streams	5-11
MTP Signaling and Audio Streams	5-12
Annunciator Signaling and Audio Streams	5-13
MOH Signaling and Audio Streams	5-14
Conferencing Resources	5-15
Software Audio Conferencing Bridge	5-16
Hardware Audio Conferencing	5-17
Conferences per Resource	5-18
Built-In Conference Resource Characteristics	5-20
Meet-Me and Ad Hoc Conferencing Characteristics	5-21
Conferencing Media Resource Configuration	5-22
Step 1a: Activate IP Voice Media Streaming Application Service	5-23
Step 1b: IP Voice Media Streaming Application Service Parameters	5-24
Step 1c: Software Conferencing Media Resource	5-25
Step 2a: Configuration of Cisco IOS Enhanced Conference Bridge in Cisco Unified Communications Manager	5-26
Step 2b and 2c: Configuration and Verification of Cisco IOS Enhanced Conference Bridge	5-28
Step 3: CallManager Service Parameters Concerning Conferencing	5-32
Meet-Me Conference Configuration	5-34
Step 2: Configure a Meet-Me Number or Pattern	5-35
MOH Essentials	5-37
MOH Sources	5-38
Unicast MOH	5-40
Multicast MOH	5-41
MOH Audio Source Selection	5-42
MOH Configuration	5-43
Step 1: Capacity Planning	5-44
Step 2a: MOH Audio File Management	5-46
Step 2b: MOH Audio Sources Configuration: MOH Audio Source	5-47
Step 2b: MOH Audio Sources Configuration: Fixed MOH Audio Source	5-48
Step 3: MOH Server Configuration	5-49
Step 4: MOH Service Parameters	5-50
Step 5a: Multicast MOH – Audio Sources Configuration	5-51
Step 5b: Multicast MOH – MOH Server Configuration	5-52
Annunciator Essentials	5-54
Annunciator Features and Capacities	5-55
Annunciator Performance	5-57
Annunciator Configuration	5-58
Media Resources Access Control Essentials	5-59
Media Resource Access Control	5-60
Media Resource Design	5-61
Media Resource Access Control Example	5-62

Media Resource Access Control Configuration	5-63
Step 1: Configure MRGs	5-64
Step 2: Configure MRGLs	5-65
Step 3: Configure Phones with MRGLs	5-66
Summary	5-67
References	5-68
Configuring Cisco Unified Communications Manager User Features	5-69
Overview	5-69
Objectives	5-69
Cisco Unified Communications Manager User Features	5-70
Call Park and Directed Call Park	5-73
Call Park Configuration	5-75
Directed Call Park	5-76
Directed Call Park Configuration	5-77
Configuration of Call Park Button	5-79
Call Pickup and Hold Reversion	5-80
Other Group Call Pickup	5-82
Call Pickup Configuration	5-83
Hold Reversion	5-85
Hold Reversion Configuration: Timer	5-86
Hold Reversion Configuration: Focus	5-89
Do Not Disturb, Intercom, and Cisco Call Back	5-90
Do Not Disturb Configuration: Common Profile	5-92
Do Not Disturb Configuration: Add DND Softkey	5-93
Intercom	5-94
Intercom Configuration Steps	5-95
Step 1: Create Intercom Partition	5-96
Step 2: Create Intercom CSS	5-97
Step 3: Create Intercom Directory Numbers	5-98
Step 4: Assign Intercom Directory Numbers to Phones	5-99
Cisco Call Back	5-101
Cisco Call Back Configuration	5-102
Barge and Privacy	5-103
Shared Line Appearance	5-105
Barge Configuration	5-106
Privacy Configuration	5-107
Privacy Display	5-108
User Options Web Pages	5-109
User Options Web Page: Phone to User Relation	5-110
User Options Example	5-111
Cisco IP Phone Services	5-112
Cisco IP Phone Services	5-114
Cisco IP Phone Services Configuration Steps	5-116
Configure Cisco IP Phone Services – Step 2: Phone Services	5-118
Configure Cisco IP Phone Services – Step 3: Parameters	5-119
Summary	5-120
References	5-120
Configuring Cisco Unified Presence-Enabled Speed Dials and Lists	5-121
Overview	5-121
Objectives	5-121
Cisco Unified Presence Essentials	5-122
Cisco Unified Communications Manager Presence Characteristics	5-123
Cisco Unified Communications Manager Presence Operation	5-124
Cisco Unified Presence Support in Cisco Unified Communications Manager	5-125
Watching Presence Status on Cisco IP Phones	5-126
Cisco IP Phones That Support Viewing Presence Status	5-127
Cisco Unified Presence Configuration	5-128
Step 1: Customizing Phone Button Templates	5-129
Step 2: Applying the Phone Button Template to IP Phones	5-130

Step 3: Configuring Cisco Unified Presence-Enabled Speed-Dial Buttons	5-131
Enabling Cisco Unified Presence-Enabled Call Lists	5-132
Enabling Cisco Unified Presence on SIP Trunks	5-133
Cisco Unified Presence Policies	5-134
Subscribe CSS and Partitions	5-135
Subscribe CSS and Partition Considerations	5-136
Subscribe CSS and Partition Considerations: Sample Scenario	5-137
Presence Policy Example: Subscribe CSS	5-138
Presence Groups	5-139
Presence Policy Example: Presence Groups	5-140
Interaction of Presence Groups, Partitions, and Subscribe CSSs	5-141
Cisco Unified Presence Policy Configuration	5-142
Implementing Presence Policies Based on Partitions and CSS:	5-143
Step 3 – Assigning Subscribe CSSs to Phones and SIP Trunks	5-143
Implementing Presence Policies Based on Presence Groups:	5-144
Step 1 – Configuring Presence Groups	5-144
Step 2: Setting the Default Inter-Presence Group Policy	5-145
Step 3a: Assigning Presence Groups to Lines and Phones	5-146
Step 3b: Assigning a Presence Group to a SIP Trunk	5-147
Summary	5-148
References	5-148
Integrating Cisco Unified Communications Manager with Voice-Mail Systems	5-149
Overview	5-149
Objectives	5-149
Cisco Unified Communications Manager Voice-Mail Integration Essentials	5-150
Third-Party Voice-Mail Systems	5-151
Cisco Unified Communications Manager and Cisco Unity Integration Using SCCP	5-153
Cisco Unity Outside Caller Call Flow	5-154
Cisco Unity Subscriber Call Flow	5-156
Voice-Mail Integration Parameters	5-157
Voice Mail Integration Elements: Incoming Call	5-158
Voice Mail Integration Elements: Listen to Messages	5-159
Cisco Unity Components	5-160
Cisco Unity Standard Features	5-161
Cisco Unity Release 5.0 Additional Features	5-164
Cisco Unified Communications Manager Configuration for Voice-Mail Integration	5-165
Interaction of Configuration Elements: Calls To Voice Mail	5-167
Interaction of Configuration Elements: Calls From Voice Mail	5-170
SCCP Voice-Mail Integration Configuration Procedure	5-172
Step 1: Create MWI Extensions	5-173
Step 2: Create Voice-Mail Ports	5-174
Step 3: Create Line Group	5-176
Step 4: Create Hunt List	5-177
Step 5: Create Hunt Pilot	5-178
Step 6: Configure Voice-Mail Pilot	5-179
Step 7: Configure Voice-Mail Profile	5-180
Cisco Unified Communications Manager Phone Configuration for Voice-Mail Usage	5-182
Cisco Unity Configuration for Cisco Unified Communications Manager Integration	5-184
Step 1: Launch Integration Tool	5-185
Step 2: SCCP Cisco Unified Communications Manager Integration	5-186
Step 3: SCCP Cisco Unified Communications Manager Integration	5-187
Step 4: Update Cisco Unity-Unified Communications Manager TSP	5-194
Cisco Unity Subscriber Configuration	5-195
Create New User Example	5-196
Summary	5-197
References	5-198
Implementing Cisco Unified Video Advantage	5-199
Overview	5-199
Objectives	5-199

Cisco Unified Video Advantage Overview	5-200
Cisco Unified Video Advantage Components	5-201
Cisco Unified Video Advantage Component Interaction	5-202
Cisco Unified Video Advantage Supported Multimedia Standards	5-203
Cisco Unified Video Advantage Communication Flows	5-204
How Calls Work with Cisco Unified Video Advantage	5-207
Video Call Bandwidth for Audio and Video Channels	5-209
Cisco Unified Video Advantage Configuration in Cisco Unified Communications Manager	5-211
Step 1: Setting the Maximum Audio Codec and Video Call Speed Allowed Per Video Call	5-212
Step 2: Setting the Maximum Allowed Bandwidth Used by Video Calls for Locations	5-213
Step 3: Required Phone Configuration Settings for Video Support	5-215
Step 4: Verification of Phone Configuration	5-216
Cisco Unified Video Advantage Installation	5-217
Step 1: Cisco Unified Video Advantage Hardware Requirements	5-218
Step 2: Cisco Unified Video Advantage Software Requirements	5-220
Step 3a: Cisco Unified Video Advantage Installation – Preparation Checklist	5-221
Step 3b: Cisco Unified Video Advantage Installation	5-222
Cisco Unified Video Advantage Verification Tools	5-224
Cisco Unified Video Advantage Verification of Camera	5-225
Active Call Verification with the Diagnostic Tool	5-226
Summary	5-227
References	5-227
Module Summary	5-228
References	5-229
Module Self-Check	5-230
Module Self-Check Answer Key	5-236

Module 4

Single-Site Off-Net Calling

Overview

Cisco Unified Communications Manager automatically routes calls to destinations within the same cluster. In order to enable off-net calls, such as to the public switched telephone network (PSTN), gateways have to be implemented and special dial plan requirements have to be considered.

This module describes how to configure Media Gateway Control Protocol (MGCP) gateways and how to create a dial plan providing endpoint addressing, path selection, calling privileges, digit manipulation, and call coverage for single-site Cisco Unified Communications Manager deployments.

Module Objectives

Upon completing this module, you will be able to implement PSTN access in Cisco Unified Communications Manager and to build a dial plan in a single-site Cisco Unified Communications Manager deployment. This ability includes being able to meet these objectives:

- Describe the implementation of MGCP gateways in Cisco Unified Communication Manager
- Describe and configure Cisco Unified Communications Manager numbering plans, directory numbers, route groups, route lists, route patterns, route filters, digit analysis, and urgent priority for on-net and off-net (PSTN) calls
- Describe digit manipulation elements in Cisco Unified Communications Manager and how to implement them
- Explain the need and uses for calling privileges and how to implement them in Cisco Unified Communications Manager
- Describe call coverage and how to implement it in Cisco Unified Communications Manager

Lesson 1

Implementing MGCP Gateways in Cisco Unified Communications Manager

Overview

Cisco Unified Communications Manager deployments need a connection to the public switched telephone network (PSTN) to place external calls. Such connections are provided by gateways which interconnect traditional telephony interfaces such as digital or analog trunks and VoIP domains. Gateways can use different protocols for signaling on VoIP call legs. Media Gateway Control Protocol (MGCP) is one of the protocols supported by Cisco Unified Communications Manager.

The purpose of this lesson is to describe the role and implementation of MGCP gateways to provide PSTN access to a Cisco Unified Communications Manager environment.

Objectives

Upon completing this lesson, you will be able to describe the implementation of MGCP gateways in Cisco Unified Communications Manager. This ability includes being able to meet these objectives:

- Describe how gateway interfaces can be controlled by Cisco Unified Communications Manager using MGCP
- Describe how Cisco Unified Communications Manager and Cisco IOS gateways support MGCP protocols
- Describe how to configure an MGCP gateway in Cisco Unified Communications Manager
- Describe how to configure a gateway for MGCP

Cisco Unified Communications Manager and MGCP Gateways

This topic describes MGCP, how the protocol functions, and how it is implemented in Cisco Unified Communications Manager.

MGCP Gateways

- MGCP (defined under RFC 2705) is a master-slave protocol
- Allows a call control device (such as Unified CM) to take control of a specific port on a gateway
- Provides centralized gateway administration and highly scalable gateway solutions:
 - Allows complete control of the dial plan from Unified CM
 - Allows Unified CM per-port control of gateway connections to PSTN, legacy PBX/VM systems, analog phones, etc.
- Allows use of plain-text commands between the Unified CM and the gateway over UDP port 2427
- Gateway must be supported by Unified CM for MGCP (use Cisco Software Advisor tool to verify compatibility)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-4

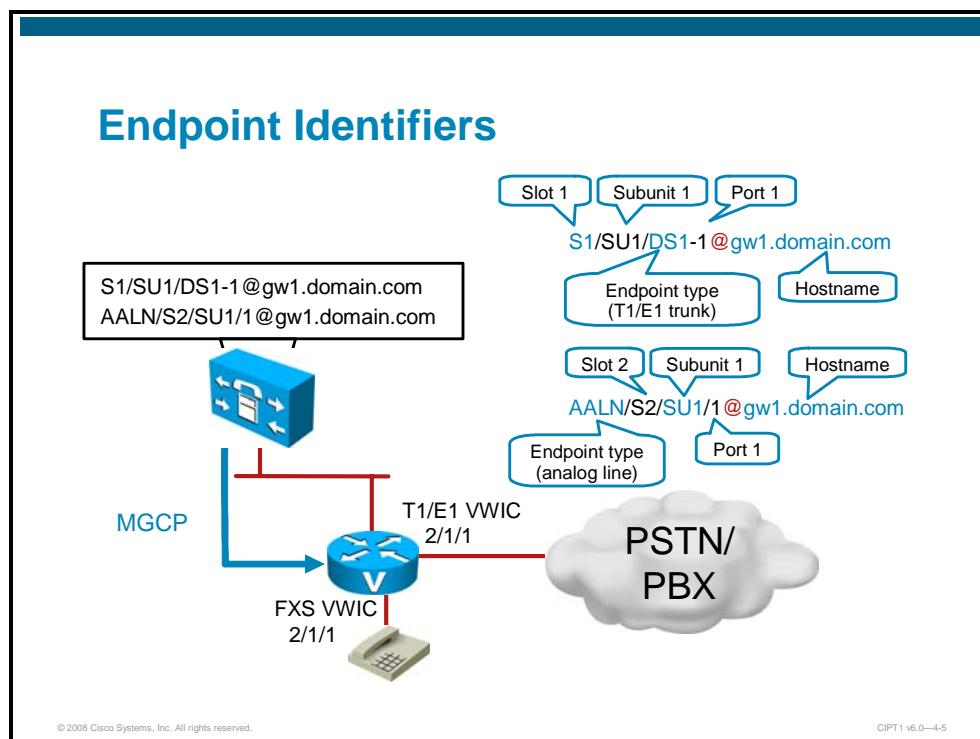
MGCP is a plain-text protocol used by call control devices to manage IP telephony gateways.

MGCP (defined under RFC 2705) is a master-slave protocol that allows a call control device, such as Cisco Unified Communications Manager, to take control of a specific port on a gateway. This has the advantage of centralized gateway administration and provides for largely scalable IP telephony solutions. With this protocol, the Cisco Unified Communications Manager knows and controls the state of each individual port on the gateway. It allows complete control of the dial plan from Cisco Unified Communications Manager, and gives Cisco Unified Communications Manager per-port control of connections to the PSTN, legacy PBX, voice-mail systems, plain old telephone service (POTS) phones, and so on. MGCP is implemented by a series of plain-text commands sent over User Datagram Protocol (UDP) port 2427 between the Cisco Unified Communications Manager and the gateway.

For an MGCP interaction to take place with Cisco Unified Communications Manager, the gateway must have Cisco Unified Communications Manager support. Use the Cisco Software Advisor tool to make sure that the platform and the version of Cisco IOS Software or Cisco Catalyst operating system is compatible with Cisco Unified Communications Manager for MGCP.

Endpoint Identifiers

This subtopic describes how identifiers are associated with an endpoint.

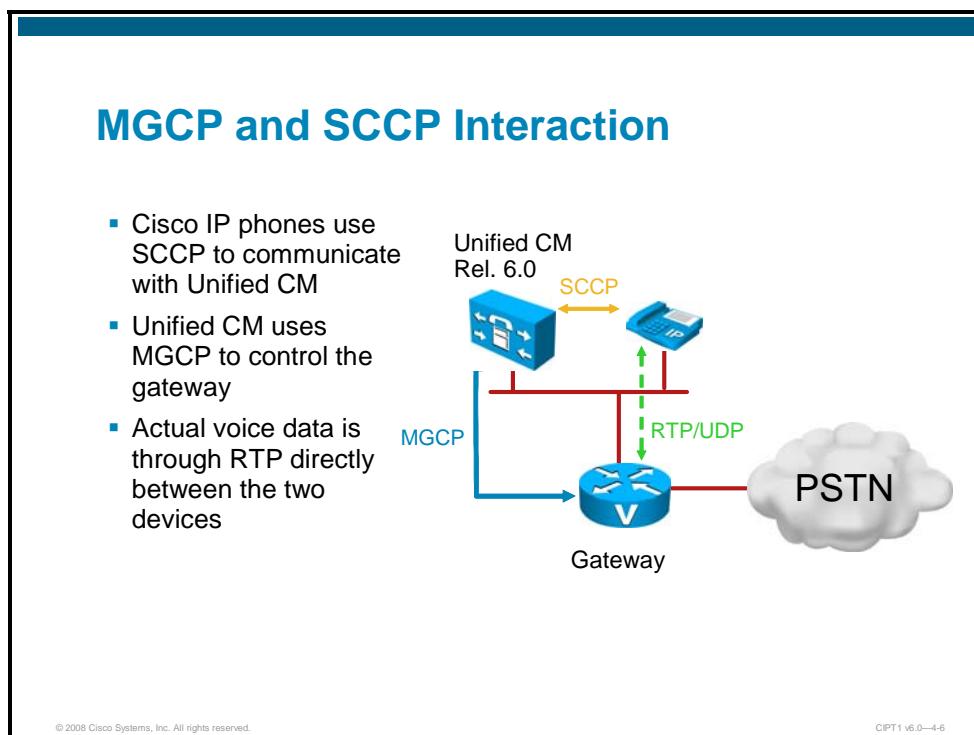


When interacting with a gateway, the call agent directs its commands to the gateway for the purpose of managing an endpoint or a group of endpoints. An endpoint identifier, as its name suggests, identifies endpoints.

Endpoint identifiers consist of two parts: a local name of the endpoint in the context of the gateway and the domain name of the gateway itself. The two parts are separated by an “at” sign (“@”). If the local part represents a hierarchy, the subparts of the hierarchy are separated by a slash (/). In the figure, the local ID may be representative of a particular “gateway/circuit #”, and the “circuit #” may in turn be representative of a “circuit ID/channel #”.

MGCP and SCCP Interaction

This subtopic describes the interactions between Cisco Unified Communications Manager, Skinny Client Control Protocol (SCCP) phones, and an MGCP gateway.



Both MGCP and SCCP are master-slave protocols; the Cisco Unified Communications Manager is the master server for both protocols. The interactions are as follows:

- IP phones communicate directly with Cisco Unified Communications Manager for all call setup signaling.
- MGCP gateways communicate directly with Cisco Unified Communications Manager for all call setup signaling.
- Actual voice traffic flows directly between the IP phone and the MGCP gateway through Real-Time Transport Protocol (RTP) over UDP.

MGCP Gateway Support in Cisco Unified Communications Manager and Cisco IOS Gateways

This topic describes how MGCP gateways are supported in Cisco Unified Communications Manager.

MGCP Support in Cisco Unified Communications

- Wide range of supported Cisco IOS router platforms
- Wide range of supported analog and digital interfaces
- Wide range of analog and digital features
- Cisco Unified Communications Manager configuration server
 - Cisco IOS MGCP gateway can pull its configuration from Cisco Unified Communications TFTP server
 - Eliminates the need for manual gateway configuration
- PRI backhaul support
 - For Cisco IOS gateways with ISDN PRIs
 - Cisco Unified Communications Manager takes control of ISDN D channel

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-8

MGCP support in Cisco Unified Communications Manager includes a wide range of analog and digital interfaces that can be used on several Cisco IOS router platforms.

Cisco Unified Communications Manager allows the Cisco IOS MGCP gateway to pull its MGCP-related configuration from the Cisco TFTP server. This eliminates the need for manual MGCP gateway configuration.

Cisco Unified Communications Manager also supports PRI backhauling. With PRI backhauling, which is supported on ISDN PRI, the MGCP call agent (that is, Cisco Unified Communications Manager) takes control of the ISDN data channel (D channel).

Supported MGCP hardware

Gateway	Supported Voice Hardware	Remarks
Cisco 3800	Analog FXS/FXO, T1 CAS (E&M Wink Start; Delay Dial only), T1/E1 PRI	Beginning with Cisco IOS Release 12.3.11T
Cisco 2800	Same as Cisco 3800	Beginning with Cisco IOS Release 12.3.8T4
Cisco 3700	Same as Cisco 3800	
Cisco 3640 and 3660	Same as Cisco 3800	
Cisco 2600/2600XM/VG200	Same as Cisco 3800	
Cisco 1751 and 1760	Same as Cisco 3800	
WS-X4604-GWY Module	Same as Cisco 3800	
Comm. Media Module (CMM)	T1 CAS FXS, T1/E1 PRI, FXS	
WS-X6608-x1 Module and FXS Module WS-X6624	T1 CAS E&M, T1 CAS FXS, T1/E1 PRI, FXS with WS-6624	
VG224	FXS only	
Cisco ATA 188	FXS only	

Supported MGCP analog features

Gateway	FXS	FXO	E&M	FXO, Battery Reversal	Analog DID	CAMA 911
Cisco 3800	Yes	Yes	No	Yes	No	No
Cisco 2800	Yes	Yes	No	Yes	No	No
Cisco 3700	Yes	Yes	No	Yes	No	No
Cisco 3640 and 3660	Yes	Yes	No	Yes	No	No
Cisco 2600 and 2600XM	Yes	Yes	No	Yes	No	No
VG200	Yes	Yes	No	Yes	No	No
Cisco 1751 and 1760	Yes	Yes	No	Yes	No	No
WS-X4604-GWY Module	Yes	Yes	No	No	No	No
Communications Media Module (CMM) 24FXS	Yes	N/A	N/A	N/A	N/A	N/A
FXS Module WS-X6624	Yes	N/A	N/A	N/A	N/A	N/A
VG224	Yes	N/A	N/A	N/A	N/A	N/A
Cisco ATA 188	Yes	N/A	N/A	N/A	N/A	N/A

Supported MGCP digital features

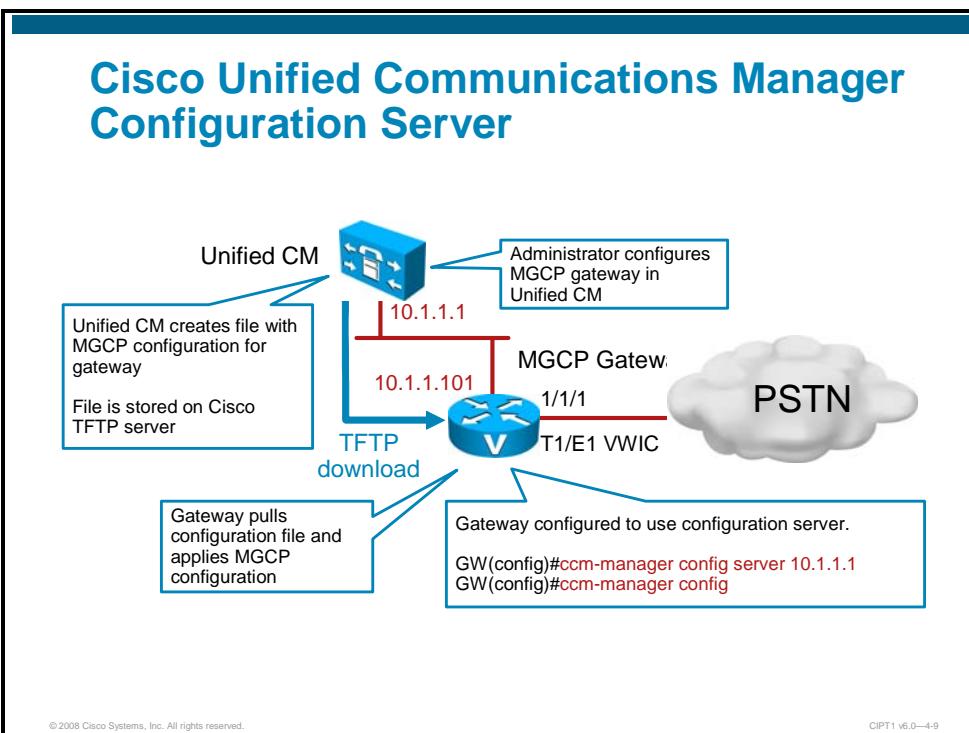
Gateway	BRI1	TI CAS (E&M)	T1 PRI	T1 QSIG	E1 PRI	E1 QSIG
Cisco 3800	12.4(2)T	Yes2	Yes2	Yes2	Yes2	Yes2
Cisco 2800	12.4(2)T	Yes2	Yes2	Yes2	Yes2	Yes2
Cisco 3700	12.4(2)T	Yes2	Yes2	Yes2	Yes2	Yes2
Cisco 3640 and 3660	12.4(2)T	Yes2	Yes2	Yes2	Yes2	Yes2
Cisco 2600 and 2600XM	12.4(2)T	Yes2	Yes2	Yes2	Yes2	Yes2
VG200	No	Yes	Yes	Yes	Yes	Yes
Cisco 1751 and 1760	12.3(14)T	Yes	Yes	Yes	Yes	Yes
WS-X4604-GWY Module	No	Yes	Yes	Yes	Yes	Yes
Communications Media Module (CMM) 6T1/E1	N/A	Yes	Yes	Yes	Yes	Yes
WS-X6608-T1/E1	N/A	Yes	Yes	Yes	Yes	Yes

Note

1. Cisco IOS Release 12.4(2)T supports BRI MGCP with the following hardware: NM-HDV2, NM-HD-XX, and on-board HWIC slots. BRI MGCP is also supported on older Cisco IOS releases with NM-1V/2V hardware.
2. AIM-VOICE-30 modules require Cisco IOS Release 12.2.13T.

Cisco Unified Communications Manager Configuration Server

This subtopic describes the Cisco Unified Communications Manager configuration server feature in conjunction with a Cisco IOS gateway.



When using the Cisco Unified Communications Manager configuration server feature, gateway- and interface-specific MGCP configuration commands are provided by Cisco Unified Communications Manager in the form of an Extensible Markup Language (XML) configuration file that is downloaded by the Cisco IOS gateway from the Cisco Unified Communications Manager TFTP server. This is the recommended approach to integrate Cisco IOS MGCP gateways with Cisco Unified Communications Manager.

When you configure MGCP gateways to support Cisco Unified Communications Manager, a Cisco Unified Communications Manager TFTP server is used to allow the download of gateway configuration commands contained in XML files. Each MGCP gateway in the network has an associated gateway-specific configuration that is stored in the centralized TFTP directory. A tailored XML file can be created and downloaded from the TFTP server to a designated MGCP gateway.

When changes are made to the configuration in the Cisco Unified Communications Manager database, a message is sent by Cisco Unified Communications Manager to the affected MGCP gateway, instructing the gateway devices to download the updated XML configuration file. Each device has an XML parser that interprets the XML file according to its device-specific requirements. Cisco MGCP gateways, for example, translate the content of the XML file into specific Cisco IOS commands for local execution.

PRI Backhaul

This subtopic explains PRI backhaul, which is an important concept in implementing ISDN PRI on an MGCP gateway.

PRI Backhaul

- D-channel call-setup signals need to be carried in their raw form back to the Unified CM to be processed
- Gateway terminates data link layer and passes the rest of signals (Q.931 and above) to Unified CM via TCP port 2428
- D-channel will be down unless it can communicate with Unified CM

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-10

A PRI backhaul is an internal interface between Cisco Unified Communications Manager and Cisco MGCP gateways (that is, a separate channel for backhauling signaling information). It forwards Layer 3 PRI (Q.931) backhauls over a TCP connection. Layer 3 information is forwarded independent of the native protocol used on the PSTN time-division multiplexing (TDM) interface.

A PRI is distinguished from other interfaces by the fact that data received from the PSTN on the D-channel must be carried in its raw form back to the Cisco Unified Communications Manager to be processed. The gateway does not process or change this signaling data, it simply passes it onto the Cisco Unified Communications Manager through TCP port 2428. The gateway is still responsible for the termination of the Layer 2 data. That means that all the Q.921 data link layer connection protocols are terminated on the gateway, but everything above that (Q.931 network layer data and beyond) is passed onto the Cisco Unified Communications Manager. This also means that the gateway does not bring up the D-channel unless it can communicate with Cisco Unified Communications Manager to backhaul the Q.931 messages contained in the D-channel. The figure illustrates these relationships.

MGCP Gateway Configuration in Cisco Unified Communications Manager

This topic describes the configuration steps for implementing an MGCP gateway in Cisco Unified Communications Manager.

Cisco Unified Communications Manager Gateway Configuration Procedure

1. Add an MGCP gateway.
2. Configure the MGCP gateway.
3. Add voice modules.
4. Add VICs to the module.
5. Configure MGCP endpoints.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-12

MGCP gateway implementation includes configuration steps on *both* Cisco Unified Communications Manager (the MGCP call agent) and the MGCP gateway that will be controlled.

The steps to configure an MGCP gateway differ depending on the type of MGCP gateway platform selected.

The high-level Cisco Unified Communications Manager configuration steps for implementing an MGCP gateway are as follows:

- Step 1** Add the MGCP gateway to Cisco Unified Communications Manager.
- Step 2** Configure the MGCP gateway in Cisco Unified Communications Manager.
- Step 3** Add one or more voice modules to the slots of the MGCP gateway in Cisco Unified Communications Manager.
- Step 4** Add voice interface cards (VICs) to the configured modules.
- Step 5** Configure the MGCP endpoints (one or more per VIC).

Step 1: Add an MGCP Gateway

First, add a new MGCP gateway to the Cisco Unified Communications Manager.

Step 1: Add an MGCP Gateway

Add a new Gateway

Next

Select the type of gateway you would like to add:

Gateway Type * -- Not Selected --
-- Not Selected --
Cisco IAD2400
Cisco 1751
Cisco 1760
Cisco 269X
Cisco 26XX
Cisco 2800
Cisco 2811
Cisco 2821
Cisco 2851
Cisco 362X
Cisco 364X
Cisco 366X
Cisco 3725
Cisco 3745
Cisco 3825
Cisco 3845
Cisco Catalyst 4000 Access Gateway Module
Cisco Catalyst 4224 Voice Gateway Switch
Cisco Catalyst 6000 24 port FXS Gateway

* - indicates required field

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-13

Follow these configuration steps to add an MGCP gateway to Cisco Unified Communications Manager:

- Step 1** From Cisco Unified Communications Manager Administration, choose **Device > Gateway**.
- Step 2** Click the **Add New** button. The Add a New Gateway window displays.
- Step 3** From the **Gateway Type** drop-down list box, choose the appropriate MGCP gateway.
- Step 4** Click **Next**.

Step 1: Add an MGCP Gateway (Cont.)

Add a new Gateway

Next

Select the type of gateway you would like to add:

Gateway Type Cisco 2811

Protocol*

-- Not Selected --
-- Not Selected --
MGCP
SCCP

10. Select MGCP for the gateway protocol.

11. Click **Next**.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-14

Step 5 If a Protocol drop-down list box displays, choose MGCP and click **Next**.

Note Some gateways support SCCP and MGCP. Only when adding such a gateway, the protocol list box appears.

Step 2: MGCP Gateway Configuration

After the MGCP gateway has been added, the gateway configuration page displays.

The screenshot shows the 'Step 2: MGCP Gateway Configuration' page. At the top right is a 'Save' button. Below it is a 'Status' section with a message 'Status: Ready'. The 'Gateway Details' section includes fields for 'Product' (Cisco 2811) and 'Protocol' (MGCP). The 'Domain Name*' field is highlighted with a red box and contains 'HQ-1'. The 'Description' field contains 'Headquarters MGCP Gateway'. The 'Cisco Unified Communications Manager Group*' dropdown is also highlighted with a red box and shows 'Default'. Below this is a 'Configured Slots, VICs and Endpoints' section with dropdowns for 'Module in Slot 0' and 'Module in Slot 1', both showing '< None >'. The 'Product Specific Configuration Layout' section contains fields for 'Global ISDN Switch Type' (4ESS), 'Switchback Timing*' (Graceful), 'Switchback uptime-delay (min)' (10), 'Switchback schedule (hh:mm)' (12:00), and 'Type Of DTMF Relay*' (Current GW Config). A question mark icon is next to the 'Switchback Timing*' field. Callouts provide additional information: one points to the 'Domain Name*' field with 'Enter gateway name.', another to the 'Description' field with 'Enter description.', a third to the 'Cisco Unified Communications Manager Group*' dropdown with 'Select Cisco Unified Communications Manager Group.', a fourth to the 'Global ISDN Switch Type' field with 'Get help for global parameters', and a fifth to the 'Type Of DTMF Relay*' field with 'Configure global parameters'. At the bottom of the page are copyright notices: '© 2008 Cisco Systems, Inc. All rights reserved.' and 'CIPT1 v6.0—4-15'.

The configuration of an MGCP gateway depends on the selected platform. In the example, a Cisco IOS 2811 router is selected.

To configure an MGCP gateway, follow these steps:

- Step 1** Enter the name of the gateway in the Domain Name field. The name has to match the hostname of the Cisco IOS router.
- Step 2** Enter a description for the gateway.
- Step 3** Select a Cisco Unified Communications Manager group.
- Step 4** Configure global parameters such as the Global ISDN Switch Type.

Note In Cisco IOS routers, the ISDN switch type is configured globally and can be set to a different value per ISDN interface. The global ISDN switch type is part of the gateway configuration. The interface-specific switch type can be configured at the MGCP endpoint.

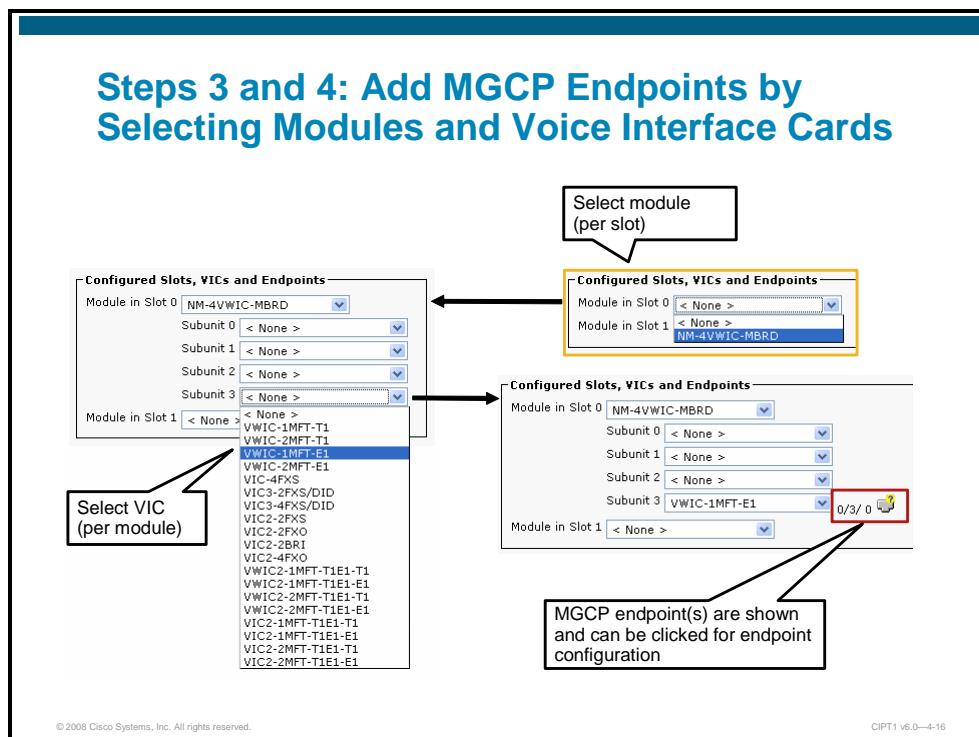
- Step 5** Click **Save** when you finish the gateway configuration.
-

Tip Help for the configuration parameters can be displayed by clicking the question mark symbol.

Note The gateway configuration parameters depend on the selected gateway.

Steps 3 and 4: Add MGCP Endpoints by Selecting Modules and VICs

Continue the configuration by adding MGCP endpoints to the MGCP gateway.



Endpoints are added by selecting voice modules and voice interface cards at the gateway configuration page. To add endpoints to a gateway, follow these steps:

Step 1 Locate the section Configured Slots, VICs and Endpoints, where the available slots are listed for the displayed gateway.

Step 2 Per slot, select the voice module that is used in the MGCP gateway.

Note Only voice modules have to be specified. If network modules are used in a slot, do not select a module.

Step 3 Click **Save** and the subunits (VIC slots) of the selected voice module will be displayed.

Step 4 Per subunit (VIC slot), select the voice interface card that is used.

Note Only voice interface cards have to be specified. If network interface cards are used in a module, do not select an interface card.

Step 5 Click **Save** and the endpoints of the selected VIC will be displayed.

Note Repeat Steps 4 and 5 for each subunit of a module. Repeat Steps 2 to 5 for each module of the gateway.

Tip	Use the Cisco IOS command show diag at the gateway to display the modules and interface cards that the gateway is equipped with. In Cisco Unified Communications Manager, modules and interface cards are listed by the product number (or field-replaceable unit [FRU]), which is part of the output of the show diag command.
------------	---

Step 5: Configure the MGCP Endpoint

Continue with the configuration of the MGCP endpoints.

Step 5: Configure the MGCP Endpoint

Device Information

Product	Cisco MGCP E1 Port
Gateway	HQ-1
Device Protocol	Digital Access PRI
End-Point Name *	S0/SU3/DS1-0@HQ-1
Description	S0/SU3/DS1-0@HQ-1
Device Pool*	-- Not Selected --
Common Device Configuration	< None >
Call Classification*	Use System Default
NetworkLocale	< None >
Packet Capture Mode*	None
Packet Capture Duration	0
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Load Information	
<input type="checkbox"/> Transmit UTF-8 for Calling Party Name	
<input type="checkbox"/> v150 (subset)	

Interface Information

PRI Protocol Type*	PRI EURO
Protocol Side*	User
Channel Selection Order*	Bottom Up
Channel IE Type*	Use Number when 1B
PCM Type*	A-law
Delay for first restart (1/8 sec ticks)*	32
Delay between restarts (1/8 sec ticks)*	4
<input checked="" type="checkbox"/> Inhibit restarts at PRI initialization	
<input type="checkbox"/> Enable status poll	
<input type="checkbox"/> Unattended Port	

Note: MGCP endpoint configuration parameters differ per type of endpoint.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—4-17

Enter endpoint description and select device pool

Verify ISDN PRI interface configuration and change if required

After you add voice modules and VICs in the Configured Slots, VICs and Endpoints section of the gateway configuration, endpoints of the VICs are displayed.

To configure an MGCP endpoint, follow these steps:

- Step 1** Click the endpoint identifier (for example, **0/3/0**).
- Step 2** If you are asked for the device protocol (such as T1 or E1 channel associated signaling [CAS] or PRI), choose the protocol that should be used on the endpoint and click **Next**.

Note The device protocol is configured only on endpoints that support multiple choices.

- Step 3** Enter a description for the endpoint.
- Step 4** Choose the device pool that should be used by this endpoint.
- Step 5** In the Interface Information section, verify the interface configuration parameters and change them if necessary.

Note The interface configuration parameters depend on the selected endpoint.

Tip Help for the configuration parameters can be displayed from **Help > This Page**.

Step 5: Configure the MGCP Endpoint (Cont.)

The screenshot shows two configuration panels side-by-side. The left panel, titled 'PRI Protocol Type Specific Information', contains several checkboxes and dropdowns. The right panel, titled 'Product Specific Configuration Layout', contains various configuration fields like Line Coding, Framing, Clock, Input Gain, Output Attenuation, Echo Cancellation Enable, and Echo Cancellation Coverage. Callouts point from three boxes at the bottom to specific parts of the interface: one points to the PRI settings, another to the product-specific layout, and a third to the help question mark icon.

PRI Protocol Type Specific Information

- Display IE Delivery
- Redirecting Number IE Delivery - Outbound
- Redirecting Number IE Delivery - Inbound
- Send Extra Leading Character in Display IE***
- Setup non-ISDN Progress Indicator IE Enable****
- MCDN Channel Number Extension Bit Set to Zero**
- Send Calling Name In Facility IE
- Interface Identifier Present**
- Interface Identifier Value**
- Connected Line ID Presentation (QSIG Inbound Call)*

Product Specific Configuration Layout

Line Coding*	HDB3
Framing*	CRC4
Clock*	External
Input Gain (-6..14 db)*	0
Output Attenuation (-6..14 db)*	0
Echo Cancellation Enable*	Enable
Echo Cancellation Coverage (ms)*	64

Note: MGCP endpoint configuration parameters differ per type of endpoint.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-18

- Step 6** Verify the PRI Protocol Type Specific Information configuration parameters and change them if required.

Note The displayed parameters depend on the selected endpoint.

- Step 7** Verify the Product Specific Configuration Layout configuration parameters and change them if required.

Tip Help for the product specific configuration parameters can be displayed by clicking the question mark symbol.

Note The displayed parameters depend on the selected endpoint.

- Step 8** Click **Save** when you finish the endpoint configuration.

Note Repeat Steps 1 to 8 for each endpoint.

Cisco IOS Gateway MGCP Configuration

This topic describes how to configure a Cisco IOS MGCP gateway to integrate with Cisco Unified Communications Manager.

Cisco IOS Gateway MGCP Configuration Overview

Recommended method (configuration server):

1. Specify the IP address of the configuration server (Unified CM TFTP server)
2. Enable configuration download
3. Optional: Modify automatically applied MGCP configuration

Alternative (manual) method:

1. Specify primary and redundant call agent (Unified CM) servers
2. Configure required global MGCP parameters
3. Enable MGCP on POTS dial peers
4. Enable MGCP

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-20

After adding the MGCP gateway in the Cisco Unified Communications Manager web administration, the MGCP gateway needs to be configured to register to the Cisco Unified Communications Manager. There are two methods of configuring a Cisco IOS-based gateway to register to Cisco Unified Communications Manager via MGCP:

■ **Cisco IOS MGCP gateway configuration by use of a configuration server:**

Step 1 Specify the IP address of the configuration server (Cisco Unified Communications Manager TFTP server).

Note If more than one Cisco Unified Communications Manager TFTP server is deployed in the Cisco Unified Communications Manager cluster, configure the gateway with all Cisco Unified Communications Manager TFTP server IP addresses.

Step 2 Enable the configuration server feature.

Step 3 If required, modify the downloaded and applied MGCP configuration.

■ **Manual Cisco IOS MGCP gateway configuration:**

Step 1 Specify the IP address of the MGCP call agent (Cisco Unified Communications Manager server).

Note If more than one Cisco Unified Communications Manager server is used for call processing (that is, running the Cisco CallManager service), configure the gateway with a primary and redundant call agent by specifying the IP addresses of two Cisco Unified Communications Manager call-processing servers.

Step 2 Configure global MGCP parameters.

Note Examples of global MGCP configuration commands are **mgcp packet** and **mgcp rtp** commands.

Step 3 Enable MGCP on POTS dial peers.

Step 4 Enable MGCP.

Note More information about manual configuration of MGCP gateways is provided in the CVOICE course.

Configuring Cisco IOS Gateway for MGCP Using a Configuration Server

This subtopic describes how to configure a Cisco IOS gateway for MGCP using a configuration server.

Configuring Cisco IOS Gateway for MGCP Using a Configuration Server

Prerequisites:

- MGCP gateway needs to be configured in Unified CM
- Gateway hostname must match name specified in Unified CM gateway configuration

```
router(config)#ccm-manager config server <CUCM_TFTP_IP>
```

- Specifies Unified CM TFTP server hosting the gateway configuration XML file

```
router(config)#ccm-manager config
```

- Enables gateway to pull configuration from TFTP server

© 2008 Cisco Systems, Inc. All rights reserved.

CPT1 v6.0—4-21

Two commands are required for a Cisco IOS MGCP gateway to pull its MGCP configuration from a configuration server (Cisco Unified Communications Manager TFTP server).

The command **ccm-manager config server {IP address or list of IP addresses}** specifies the IP addresses of the TFTP configuration server (Cisco Unified Communications Manager TFTP server). If more than one Cisco Unified Communications Manager TFTP server is deployed in the cluster, a list of IP addresses can be specified (with a space between the IP addresses). The Cisco IOS MGCP gateway will try the IP addresses in a specified order.

The command **ccm-manager config** enables the configuration server feature. Unless this command has been entered, the **ccm-manager config server** command is ignored.

In order for the configuration feature to work, the following prerequisites have to be met:

- IP connectivity between the MGCP gateway and the Cisco Unified Communications Manager TFTP servers.
- Configuration of the MGCP gateway in Cisco Unified Communications Manager.
- The hostname of the Cisco IOS MGCP gateway has to match the domain name under the Cisco Unified Communications Manager MGCP gateway configuration.

If all these conditions are met and the gateway is configured with the **ccm-manager config** and the **ccm-manager config server** commands, the gateway can download its XML configuration file from the TFTP server.

Note

The name of the configuration file is *{hostname of Cisco IOS MGCP gateway}.cnf.xml*. For example, HQ-1.cnf.xml if the hostname of the gateway is HQ-1.

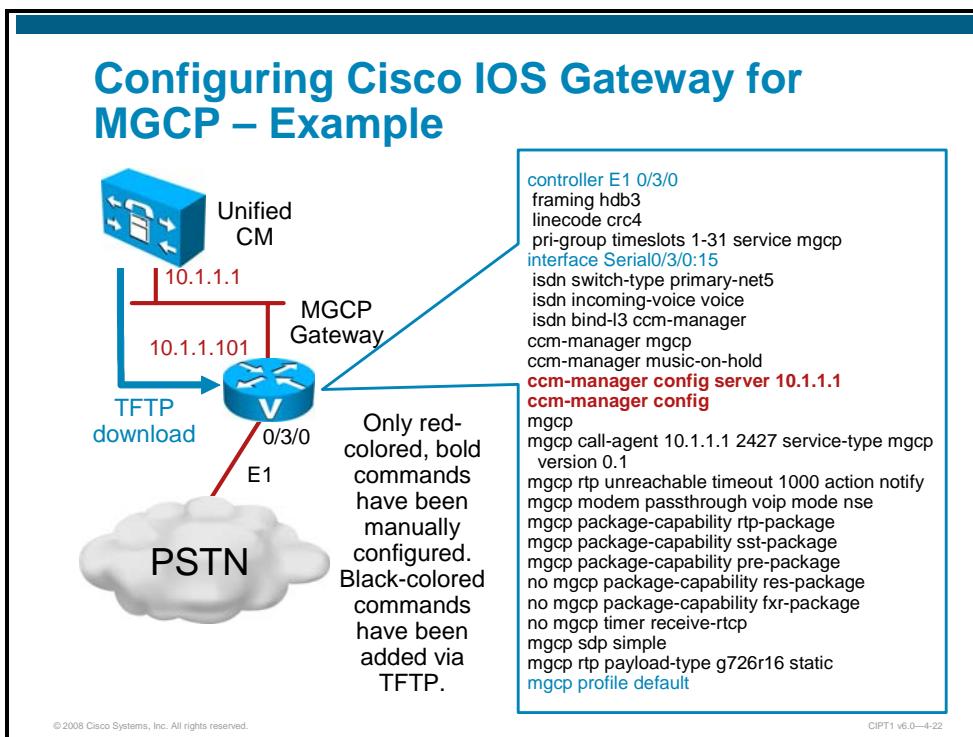
The gateway then parses the XML file, converts the information to appropriate Cisco IOS configuration commands, and configures itself for MGCP operation.

The gateway then registers with Cisco Unified Communications Manager using the MGCP protocol.

After a successful configuration download, the MGCP gateway saves the running configuration to NVRAM, which updates the startup configuration. Any manually-added configuration parameters are also saved to NVRAM if they were not previously saved. Manually-added configuration parameters are updates to the configuration that were made using the command-line interface (CLI).

Configuring Cisco IOS Gateway for MGCP – Example

The figure shows an example of a Cisco IOS MGCP gateway which pulls its configuration from a configuration server.



In the example, there is one Cisco Unified Communications Manager server (providing call processing and TFTP services) with IP address 10.1.1.1. There is a Cisco IOS MGCP gateway with a connection to the PSTN using an E1 interface (port 0/3/0). The gateway and its E1 PRI endpoint have been added to Cisco Unified Communications Manager. At the gateway, the commands **ccm-manager config server 10.1.1.1** and **ccm-manager config server** have been entered. No MGCP configuration commands have been manually entered because the MGCP configuration is automatically downloaded and applied by the configuration server feature.

After the gateway downloaded its cnf.xml configuration file from the Cisco Unified Communications Manager TFTP server, the following MGCP commands have been added and saved to NVRAM:

```
controller E1 0/3/0
framing crc4
linecode hdb3
pri-group timeslots 1-31 service mgcp
!
interface Serial0/3/0:15
isdn switch-type primary-4ess
isdn incoming-voice voice
isdn bind-l3 ccm-manager
!
ccm-manager mgcp
ccm-manager music-on-hold
!
mgcp
```

```
mgcp call-agent 10.1.1.1 2427 service-type mgcp version 0.1
mgcp rtp unreachable timeout 1000 action notify
mgcp modem passthrough voip mode nse
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp package-capability pre-package
no mgcp package-capability res-package
no mgcp package-capability fxr-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp rtp payload-type g726r16 static
```

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- MGCP provides centralized gateway administration and highly scalable gateway solutions. It allows Cisco Unified Communications Manager to take control of a specific port on a voice gateway.
- Cisco Unified Communications Manager supports various MGCP gateway router platforms and interfaces. The gateway MGCP configuration can be provided by Cisco Unified Communications Manager for TFTP download.
- To configure MGCP in Cisco Unified Communications Manager, add an MGCP gateway, add voice modules, add VICs, and then configure the VICs.
- Configure Cisco IOS MGCP gateways to pull the configuration from Cisco Unified Communications Manager to reduce manual configuration efforts.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-23

For additional information, refer to these resources:

- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1) –
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Cisco CallManager and Cisco IOS Interoperability Guide – Configuring MGCP Gateway Support for Cisco Unified Communications Manager –
http://www.cisco.com/en/US/partner/products/ps6441/products_configuration_guide_chapter09186a00805583bd.html

Lesson 2

Configuring Cisco Unified Communications Manager Call Routing Components

Overview

The dial plan is one of the key elements of an IP telephony system; it is at the very core of the user experience because it defines the rules that govern how a user reaches any destination.

Endpoint addressing and path selection are the most important components of a dial plan. This lesson describes endpoint addressing, digit analysis, and path selection in a Cisco Unified Communications Manager deployment.

Objectives

Upon completing this lesson, you will be able to describe and configure Cisco Unified Communications Manager numbering plans, directory numbers, route groups, route lists, route patterns, route filters, digit analysis, and urgent priority to place public switched telephone network (PSTN) calls. This ability includes being able to meet these objectives:

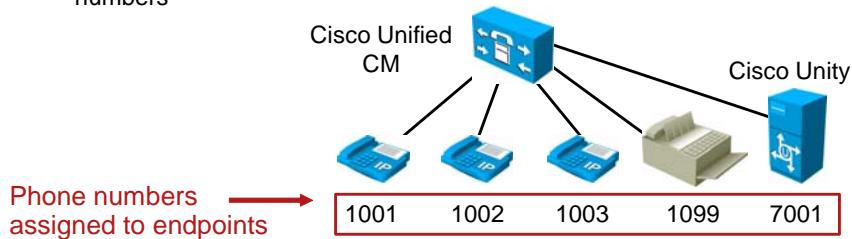
- Describe the concept of endpoint addressing, including on-net versus off-net dialing and dialing string length of uniform on-net dialing
- Describe the concept of call routing in Cisco Unified Communications Manager
- Describe how Cisco Unified Communications Manager analyzes digits
- Describe how Cisco Unified Communications Manager performs path selection
- Describe how to configure Cisco Unified Communications Manager path selection
- Describe features that relate to call routing

Endpoint Addressing

This topic describes how different endpoints can be addressed in a Cisco Unified Communications Manager dial plan.

Endpoint Addressing Characteristics

- Reachability of internal destinations is provided by assigning directory numbers
- Directory numbers are assigned to endpoints (phones, fax machines, etc.) and applications (voice mail systems, auto attendant, etc.)
- The number of extensions required generally determines the length of directory number digits
- DID numbers for inbound PSTN calls are mapped to internal directory numbers



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-4

Reachability of internal destinations is provided by assigning directory numbers to all endpoints (such as IP phones, fax machines, and analog phones) and applications (such as voice mail systems, auto attendants, and conferencing systems).

The number of dialable extensions determines the quantity of digits needed to dial extensions. For example, a four-digit abbreviated dial plan cannot accommodate more than 10,000 extensions (from 0000 to 9999). If 0 and 9 are reserved as operator code and off-net access code, respectively, the number range is further reduced to 8000 (1000 to 8999).

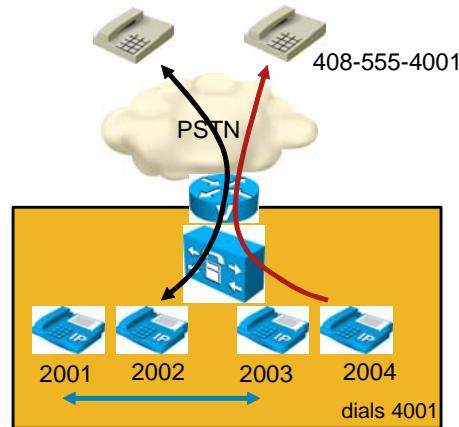
If direct inward dialing (DID) is enabled for PSTN calls, the DID numbers are mapped to internal directory numbers.

Endpoint Dialing

This subtopic describes the three types of endpoint dialing calls.

Endpoint Dialing

- **On-Net Dialing:** Calls that originate and terminate on the same telephony network (e.g., internal IP phone to IP phone calls within the same cluster)
- **Off-Net Dialing:** Calls that originate from a telephony network and terminate on a different telephony network (e.g., IP phone to PSTN calls)
- **Abbreviated Dialing:** Use of internal number to reach a PSTN phone. Unified CM maps the abbreviated number to full PSTN number



© 2008 Cisco Systems, Inc. All rights reserved.

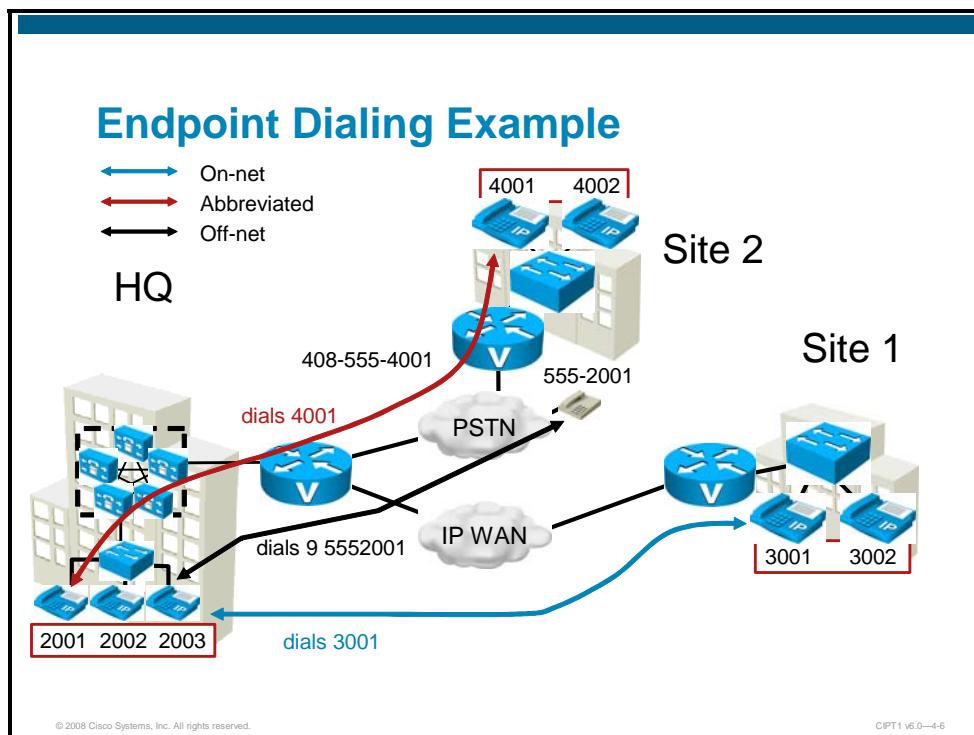
CIPT1 v6.0—4-5

The three types of endpoint dialing calls are as follows:

- **On-net dialing:** These are all calls that remain within one telephony system, such as an internal call from one IP phone to another IP phone.
- **Off-net dialing:** These are calls that are placed from one telephony system to another telephony system, such as a call from an IP phone to the PSTN.
- **Abbreviated dialing:** This is when an off-net destination is dialed by an internal number, such as when dialing a 4-digit extension to reach a colleague on his home office PSTN number. Cisco Unified Communications Manager has to map the abbreviated number to the appropriate full PSTN number in this case.

Endpoint Dialing Example

This subtopic describes an example of endpoint dialing.



In the figure, the IP phone with extension 2003, which is located in the headquarters, dials 3001 to reach an IP phone located at site 1 over the IP WAN. Because both devices are part of the same VoIP system (Cisco Unified Communications Manager) and the call is placed over the IP WAN, this call is an on-net call. The IP phone with extension 2002 dials 95552001, and the call is routed to a PSTN destination through a PSTN gateway. The call is an off-net call. The IP phone with extension 2001 dials 4001, which is an IP phone located at site 2. At site 2, Cisco Unified Communications Manager Express is used for call processing. However, in contrast to the first call, technically site 2 cannot be reached over the IP WAN but only through the PSTN. From an endpoint dialing perspective, a 4-digit extension can be dialed, which is then changed to the PSTN number 408-555-4001 by Cisco Unified Communications Manager before it is sent out through a PSTN gateway. This is an example for abbreviated dialing.

Uniform On-Net Dial Plan Example

This subtopic shows an example of a uniform on-net dial plan.

Uniform On-Net Dial Plan Example			
Range	Use	DID Ranges	Non-DID Ranges
0XXX	Excluded: 0 is used as Off-Net access code		
1XXX	Site A extensions	418 555 1 XXX	N/A
2XXX	Site B extensions	919 555 2XXX	N/A
3XXX	Site C extensions	415 555 30XX	3[1-9]XX
4[0-4]XX	Site D extensions	613 555 4[0-4]XX	N/A
4[5-9]XX	Site E extensions	450 555 4[5-9]XX	N/A
5XXX	Site A extensions	418 555 5XXX	N/A
6XXX	Site F extensions	514 555 6[0-8]XX	69XX
7XXX	Future		
8XXX	Future		
9XXX	Excluded: 9 is used as Off-Net access code		

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-7

A dial plan can be designed so that all extensions within the system are reached in a uniform way; that is, a fixed quantity of digits is used to reach a given extension from any on-net origination point. Uniform dialing is desirable because of its simplicity. A user does not have to remember different ways to dial a number when calling from various on-net locations. The figure shows an example of a 4-digit uniform on-net dial plan.

In the table in the figure, the various sites were assigned numbers in the following ways:

- Site A, the company headquarters, requires more than 1000 extensions, so two entire ranges of numbers have been retained (1XXX and 5XXX). Note that the corresponding DID ranges must also be retained from the local exchange carrier of the site.
- Site B has been assigned an entire range (2XXX), allowing for up to 1000 extensions.
- Site C was also assigned an entire range, but it has been split between 100 DID extensions (415 555 30XX) and up to 900 non-DID extensions. If growth requires more extensions for DID, any unassigned numbers from the non-DID range could be used.
- Sites D and E were each assigned 500 numbers from the 4XXX range. Note that their corresponding DID ranges must match each of the respective portions of the 4XXX range. Because the DID ranges are for different sites (probably from different PSTN service providers), more coordination effort is required to split ranges between sites. As the quantity of sites assigned within a given range increases, it becomes increasingly difficult (sometimes impossible) to make full use of an entire range.
- Site F's range is split between 900 DID numbers (6[0-8]XX) and 100 non-DID numbers (69XX).
- The ranges 7XXX and 8XXX are reserved for future use.

When an enterprise consists of few sites, such an approach can be used with few complications. The larger the enterprise, in terms of number of extensions and sites, the more of the following challenges it faces in designing a uniform dial plan:

- The number of extensions can exceed the range afforded by the quantity of digits being considered for the dial plan. For instance, if more than 8000 extensions are required (considering the exclusions of the 0XXX and 9XXX ranges), the system may require that an abbreviated dial plan use more than four digits.
- Matching on-net abbreviated extensions to DID numbers means that, when a new DID range is obtained from a local exchange carrier, it cannot conflict with the pre-existing on-net abbreviated dial ranges. For example, if the DID range of 415 555 1XXX exists in a system using a four-digit uniform abbreviated dial plan, and DID range 650 556 1XXX is also being considered, it might be desirable to increase the quantity of digits for on-net dialing to five. In this example, the five-digit on-net ranges 51XXX and 61XXX would not overlap.
- Most systems require the exclusion of certain ranges due to off-net access codes and operator dialing. In such a system, where 9 and 0 are reserved codes, no dial plan (uniform or not) could accommodate on-net extension dialing that begins with 9 or 0. This means that DID ranges could not be used if they would force the use of 9 or 0 as the first digit in the dial plan. For instance, in a five-digit abbreviated dial plan, the DID range 415 559 XXXX (or any subset thereof) could not be used. In this example, alternatives include increasing the length of the abbreviated dialing to six or more digits, or avoiding any DID range whose last five digits start with 9.

Once a given quantity of digits has been selected and the requisite ranges have been excluded (for example, ranges beginning with 9 or 0), the remaining dialing space has to be divided between all sites. Most systems require that two ranges be excluded, thus leaving eight different possibilities for the leading digit of the dial range. The table in the figure is an example of the distribution of dialing space for a typical four-digit uniform dial plan.

Cisco Unified Communications Manager Call Routing

This topic describes call routing in Cisco Unified Communications Manager.

Call Routing Types

Routing Type	Routing Component and Characteristics
Intrasite	<ul style="list-style-type: none">▪ Calls within a single site (on-net)▪ Uses assigned directory numbers to route calls internally▪ Directory numbers usually have uniform length
Intersite	<p>Calls between sites:</p> <ul style="list-style-type: none">▪ On-net: Uses internal directory numbers▪ Off-net: Uses route patterns to send calls to other site through PSTN gateway; if abbreviated dialing is used, internal number has to be translated to PSTN number first
PSTN	<p>Calls to PSTN (off-net)</p> <ul style="list-style-type: none">▪ Uses route patterns to send calls to PSTN destinations

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-9

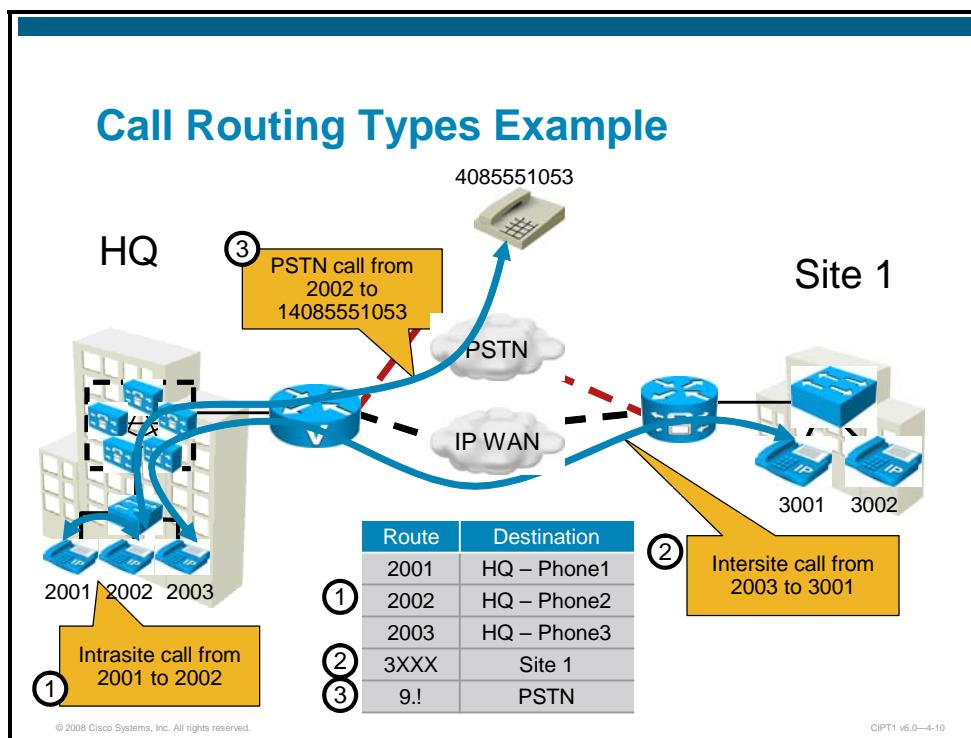
Calls need to be routed and interconnected based on the dialed number, which is similar to IP routing in that call routing is also destination-based routing. The figure shows the three major areas of call routing, as follows:

- **Intrasite routing:** Call routing within a single site
- **Intersite routing:** Call routing between multiple sites
 - Translation pattern is used for both centralized and distributed call processing deployment models
 - Route pattern is used only for distributed call processing deployment
- **PSTN routing:** Call routing between a site and the PSTN

Cisco Unified Communications Manager automatically "knows" how to route calls to internal destinations within the same cluster, because it is configured with the directory numbers of its associated devices. This can be compared to directly connected networks at a router in IP routing. For external destinations such as PSTN destinations (including off-net intersite calls, which effectively are PSTN destinations because they are addressed by their PSTN number) or other VoIP domains such as an Internet telephony service provider (ITSP) or another Cisco Unified Communications Manager cluster, an explicit route, called a route pattern, has to be configured. This is equivalent to static routes in an IP router. In summary, the call routing table of Cisco Unified Communications Manager is built of "connected" devices, consisting of directory numbers of registered IP phones and of statically entered route patterns that point to external destinations.

Call Routing Types Example

This subtopic describes an example of a simple call routing table in Cisco Unified Communications Manager.



In the example scenario in the figure, Cisco Unified Communications Manager has a basic routing table that consists of the following entries:

- 2001, 2002, and 2003 are directory numbers of phones configured in Cisco Unified Communications Manager located at the headquarters.
- There is a second site, site 1, with Cisco Unified Communications Manager Express and phones using extensions in the range of 3000–3999. To be able to route calls to this external system, Cisco Unified Communications Manager at the headquarters requires an entry in its routing table for destination 3XXX (X is a wildcard digit in route patterns) that refers to the Cisco Unified Communications Manager Express located at site 1 via a trunk.
- At the headquarters, there is a PSTN gateway. In order to route calls out to the PSTN, a route pattern 9.! (“!” is a wildcard that stands for one or more digits and “.” terminates access code 9) is configured in Cisco Unified Communications Manager that points to the headquarters PSTN gateway.

Three calls are placed, in the example:

- **2001 to 2002:** This is an internal call. The dialed number 2002 is looked up in the call routing table and the call is sent to the appropriate IP phone.
- **2002 to 914085551053:** This call is sent to the PSTN because it matches the route pattern 9!. Cisco Unified Communications Manager will be configured to strip off the PSTN access code 9 before sending the call out to the PSTN through the headquarters gateway.
- **2003 to 3001:** The dialed number 3001 matches the entry that refers to a trunk pointing to Cisco Unified Communications Manager Express at site 1. A call setup message is sent from Cisco Unified Communications Manager to Cisco Unified Communications Manager Express.

Call Routing Table Entries (Call Routing Targets)

This subtopic describes call routing table entries, or call routing targets.

Call Routing Table Entries (Call Routing Targets)

Routing Component	Description
Directory Numbers	Numbers assigned to all endpoints and applications; used for internal routing within a cluster
Translation Pattern	Used to translate a dialed number and then look up the translated number in the call routing table again
Route Pattern	Used to route calls to off-net destinations (via a gateway) or to other Unified CM clusters (via a trunk)
Hunt Pilot	Used to route calls to hunt group members based on a distribution algorithm (longest-idle, circular, etc)
Call Park Numbers	Allows placing a call on hold to a number and retrieving back the call from other phone by dialing the number
Meet-Me Numbers	Allows a conference call initiator to set up a conference call and attendees to join the conference by dialing the conference number

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-11

In the previous example, the call routing table of Cisco Unified Communications Manager was composed of directory numbers and route patterns. Additional routing components can be configured and are added to the call routing table as possible call routing targets. The table shows a list of possible call routing table entries.

All of these are possible call routing targets, which means that a dialed number can match one of these entries and the call is routed to the appropriate entity, which can be a phone line, a trunk, a gateway, a feature, or an application.

Sources of Call Routing Requests (Entities Requiring Call Routing Table Lookup)

This subtopic describes sources of call routing requests, or entities that require a call routing table lookup.

Sources of Call Routing Requests (Entities Requiring Call Routing Table Lookup)

Routing Component	Description
IP Phones	A number dialed by an IP phone is looked up in the routing table.
Trunks	A call request received through a trunk is looked up in the routing table.
Gateways	A call request received from a gateway is looked up in the call routing table.
Translation Patterns	After a translation pattern was best matched (as a target of a call routing table lookup), the transformed number is looked up again in the call routing table. The entity that generates this lookup is the translation pattern.
Voice Mail Ports	A voice mail system can be configured to allow calling other extensions or PSTN numbers (e.g., the mobile phone of an employee). In these cases, the call routing request is received from the voice mail port of Unified CM.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-12

Call routing requests that require a routing table lookup include the simplest example, an IP phone placing a call, and also calls received through gateways or trunks from the outside. In addition, the following sources of call routing requests require a routing table lookup:

- **Translation patterns:** A translation pattern is similar to a route pattern. It includes a pattern (the entry to the call routing table) and, if matched by the dialed number, another number (the translated number configured at the translation pattern) is looked up in the routing table. A translation pattern, therefore, combines both roles in a single entity: it is a call routing table target (it is matched by a dialed number) and the translation pattern causes a new, second lookup for the translated number.
- **Voice mail ports:** When a call has been sent to a voice mail system, the voice mail system can request the call to be transferred to another directory number, to a PSTN destination (such as the cell phone of a user), or to an assistant. In all these scenarios, the voice mail port is the entity that requests the call being routed by Cisco Unified Communications Manager.

Note The distinction of call routing sources and call routing targets is important when implementing features such as calling privileges, call classification, and others.

Route Patterns: Commonly Used Wildcards

This subtopic describes commonly used wildcards in a route pattern.

Route Pattern: Commonly Used Wildcards

Wildcard	Description
x	Single digit (0–9, *, #)
@	North American Numbering Plan
!	One or more digits (0–9)
[x-y]	Generic range notation
[^x-y]	Exclusion range notation
.	Terminates access code
#	Terminates interdigit timeout
<wildcard>?	Matches zero or more occurrences of any digit that matches the previous wildcard
<wildcard>+	Matches one or more occurrences of any digit that matches the previous wildcard

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-13

Route patterns can include wildcards, so that one route pattern can represent multiple numbers. This helps to keep the call routing table short and easy to interpret, similar to route aggregation in IP routing.

The table shows wildcards that can be used with route patterns, and their description.

Regarding the # wildcard, the implementation of the interdigit timeout termination is different than the implementation in Cisco IOS dial peers. In Cisco IOS dial peers, a dialed # instructs the router not to wait for additional digits. Only the digits that have been entered before the # are considered to be part of the dialed number. Therefore, the # is not included in dial-peer patterns and still can be used. The # symbol is not seen as part of the dialed number (and therefore is not searched for in a matching pattern) but rather as an *instruction* to stop waiting for additional digits. In Cisco Unified Communications Manager, the # is not only the instruction to stop digit collection but it is primarily *part of the dialed number*. Therefore, if users are to choose whether or not to use the # in order to prevent waiting for the expiration of the interdigit timeout, all route patterns have to be configured twice—once with the # and once without.

Route Pattern Examples

This subtopic describes route patterns that use wildcards, and which dialed strings each pattern matches.

Route Pattern Examples

Pattern	Result
1234	Matches 1234
1*1x	Matches numbers from 1*10 to 1*19
12xx	Matches numbers from 1200 to 1299
13[25-8]6	Matches 1326, 1356, 1366, 1376, 1386
13[^3-9]6	Matches 1306, 1316, 1326, 13*6, 13#6
13!#	Matches any number that begins with 13, is followed by one or more digits, and ends with #; 135# and 13579# are example matches

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-14

The table shows some examples of route patterns and the dialed strings that each pattern matches.

Note that the * in 1*1x is not a wildcard, but rather a dialed digit.

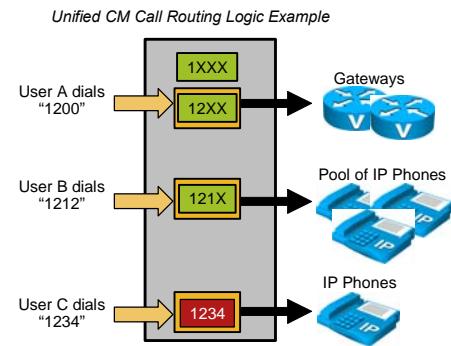
Regarding pattern 13!#, because the # symbol is used in the router pattern, it has to be dialed. Otherwise, the pattern is not matched. Therefore, if users should also be able to dial 13 followed by one or more digits without pressing the # at the end (and simply wait for the interdigit timeout to expire), an additional route pattern 13! is required.

Cisco Unified Communications Manager Call Routing Logic

When a number is dialed, Cisco Unified Communications Manager uses closest-match logic to select which pattern to match from among all the patterns in its call routing table.

Cisco Unified Communications Manager Call Routing Logic

- Unified CM uses **closest-match** logic to select the best pattern.
- When multiple matching patterns are present, the best pattern is selected based on:
 1. It matches the dialed string.
 2. It matches the fewest strings other than the dialed string.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-15

In practice, when multiple potentially matching patterns are present, the destination pattern is chosen based on the following criteria:

- It matches the dialed string.
- Among all the potentially matching patterns, it matches the fewest strings other than the dialed string. For example, consider the case shown in the figure, in which the call routing table includes the patterns 1XXX, 12XX, 121X, and 1234.

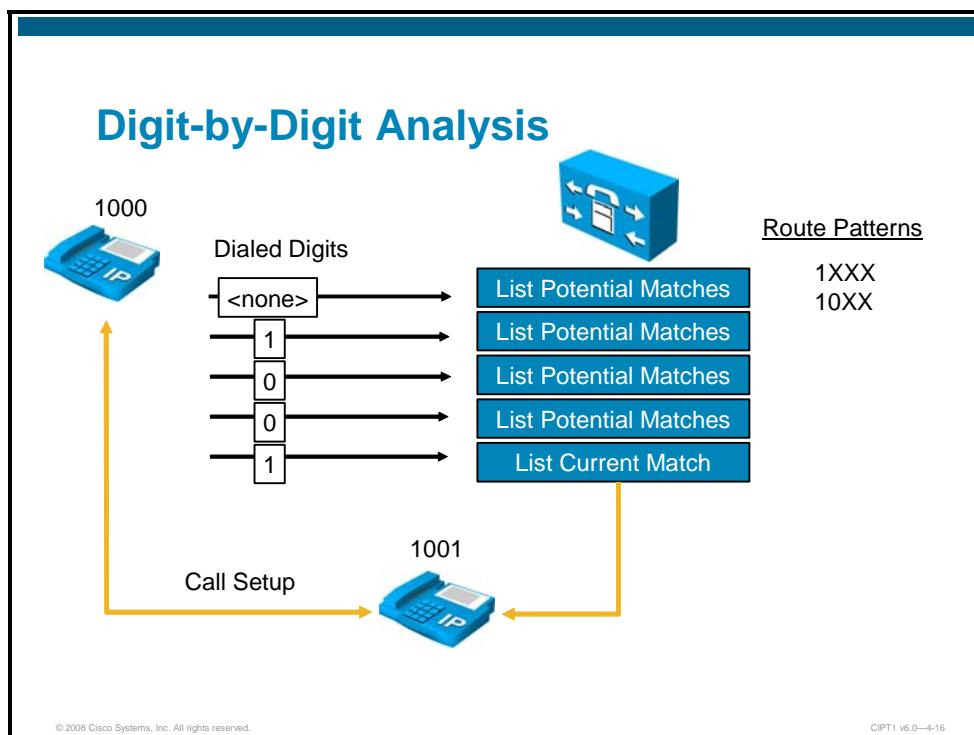
When user A dials the string 1200, Cisco Unified Communications Manager compares it to the patterns in its call routing table. In this case, there are two potentially matching patterns, 1XXX and 12XX. Both of them match the dialed string, but 1XXX matches a total of 1000 strings (from 1000 to 1999) while 12XX matches only 100 strings (from 1200 to 1299). Therefore, 12XX is selected as the destination of this call.

When user B dials the string 1212, there are three potentially matching patterns, 1XXX, 12XX and 121X. As mentioned above, 1XXX matches 1000 strings and 12XX matches 100 strings. However, 121X matches only 10 strings; therefore it is selected as the destination of the call.

When user C dials the string 1234, there are three potentially matching patterns, 1XXX, 12XX, and 1234. As mentioned above, 1XXX matches 1000 strings and 12XX matches 100 strings. However, 1234 matches only a single string (the dialed string); therefore it is selected as the destination of this call.

Digit-by-Digit Analysis

Cisco Unified Communications Manager analyzes incoming dialed digits one-by-one, as shown in the figure.



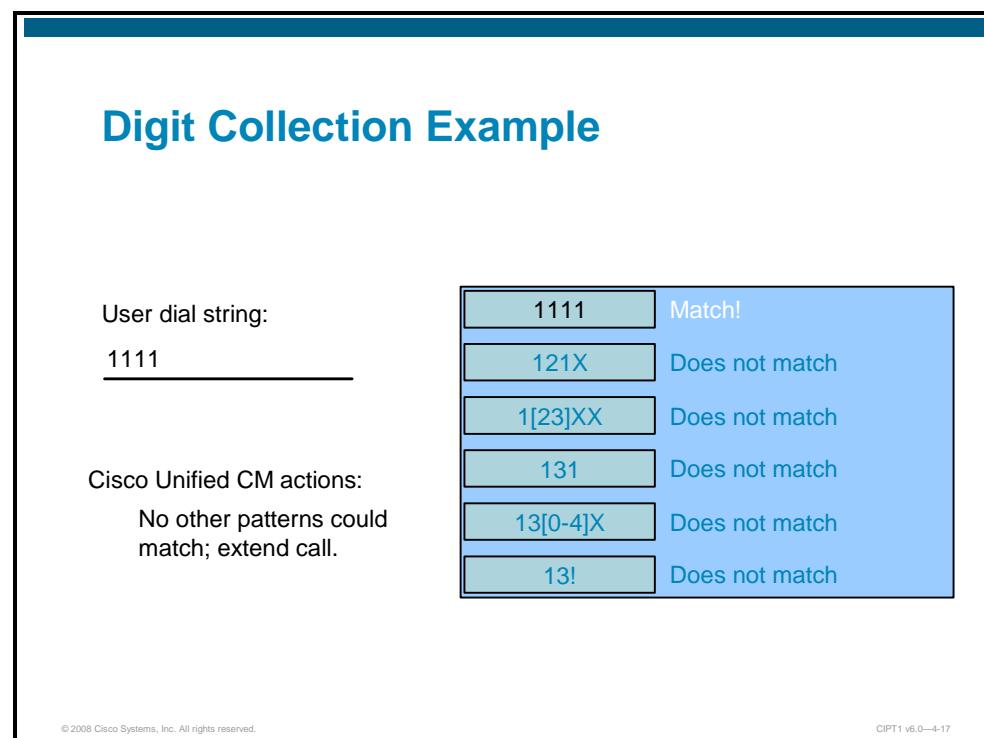
If an endpoint sends dialed digits one-by-one, Cisco Unified Communications Manager starts digit analysis immediately when it receives the first digit. In fact, digit analysis starts even one step before, when a phone indicates an off-hook state to Cisco Unified Communications Manager. Cisco Unified Communications Manager looks up a null string dialed number which matches all available call routing tables at this point.

By each additional digit received, Cisco Unified Communications Manager can reduce the list of potential matches (that is, the entries of the call routing tables that match the digits received so far). Once a single entry is matched, such as the directory number 1001 in the example, the so-called “current match” is used and the call is sent to the corresponding device.

Note	Cisco Unified Communications Manager does not always receive dialed digits one-by-one. Skinny Client Control Protocol (SCCP) phones always send digit-by-digit, session initiation protocol (SIP) phones can use en bloc dialing to send the whole dialed string at once, or Keypad Markup Language (KPML) to send digit-by-digit. If digits are received en bloc, the whole received dial string is checked against the call routing table at once.
-------------	--

Digit Collection Example

This subtopic describes digit collection in Cisco Unified Communications Manager.

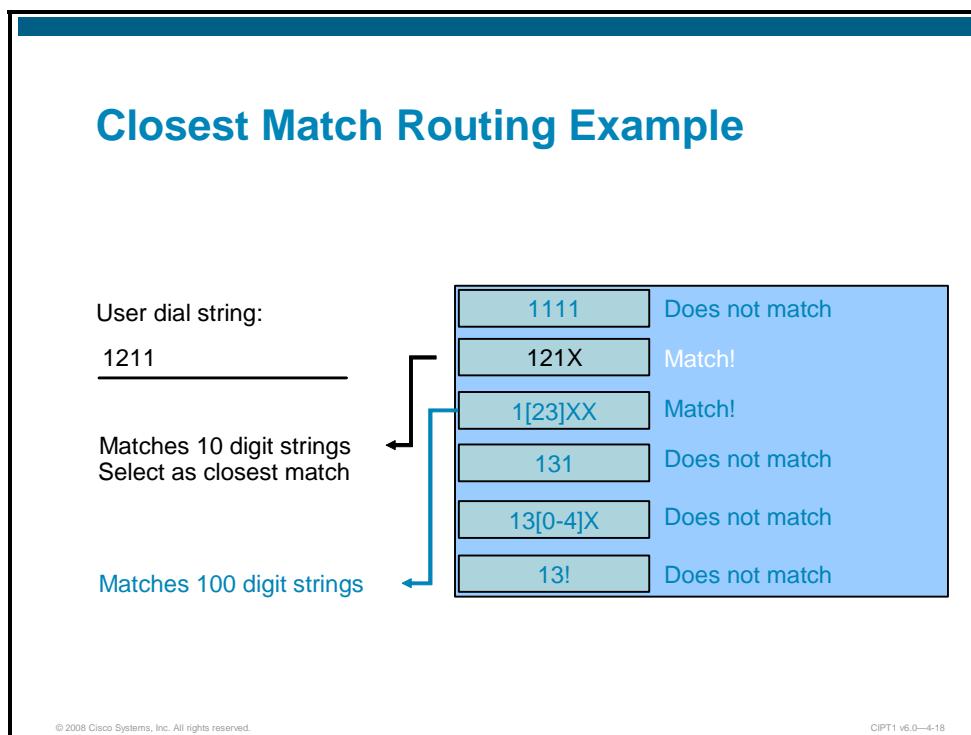


The figure shows an example of digit collection in Cisco Unified Communications Manager.

Digit collection is stopped as soon as an entry in the call routing table is matched in its full length and no other potential matches exist. In the example, a user dials 1111. Cisco Unified Communications Manager interprets the number digit-by-digit. After the first two digits have been analyzed, only one potential match is left, the first entry, because all other entries in the call routing table require a different digit than 1 at the second position. Cisco Unified Communications Manager continues collecting digits until it receives four digits (1111); now the first entry is fully matched and is used to route the call.

Closest Match Routing Example

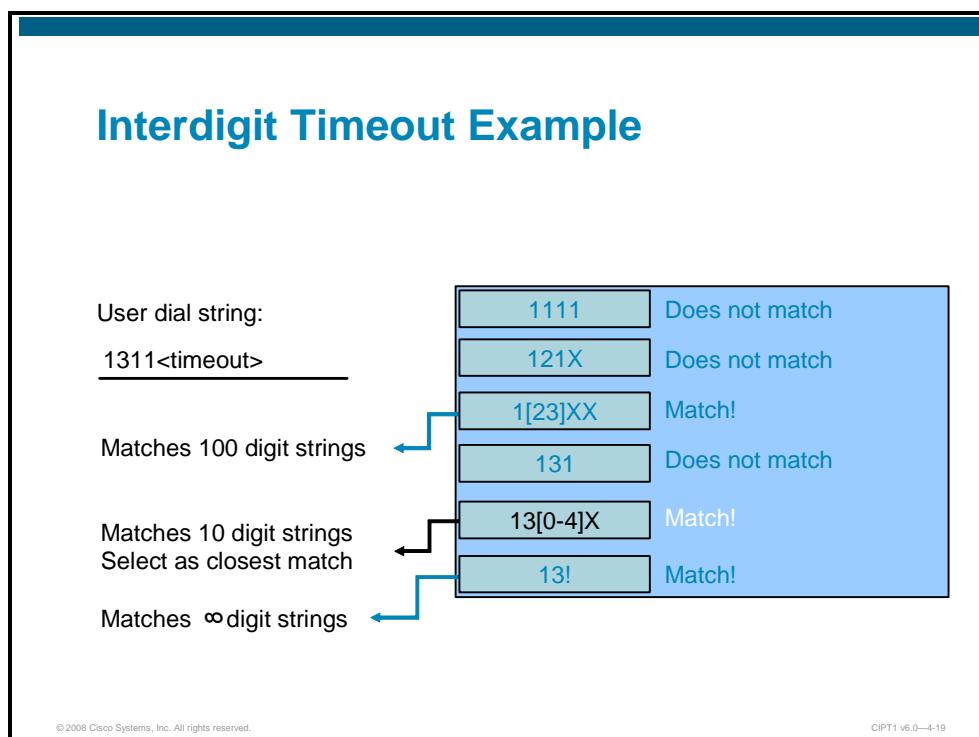
The figure illustrates how Cisco Unified Communications Manager selects a call routing table entry if multiple entries match the dialed number.



In the example, the user dials 1211. After interpreting these digits, Cisco Unified Communications Manager has two matches: 121X and 1[23]XX, and no additional potential matches. Therefore, digit collection is stopped and the best-match logic applied. Route pattern 121X stands for 10 possible numbers, while route pattern 1[23]XX matches 100 numbers that start with 12. Therefore, the first entry is the best matching entry and will be used to route the call.

Interdigit Timeout Example

The figure shows an example in which the interdigit timeout has to expire before Cisco Unified Communications Manager can make its call routing decision.



In this example, a user dials 1311. Cisco Unified Communications Manager has two potential matches: 13[0-4]X and 13!. Because the second entry is a variable-length pattern, Cisco Unified Communications Manager has to wait for additional digits provided by the user. After the interdigit timer expires, it is clear that both pattern match and Cisco Unified Communications Manager have to route the call based on best-match logic, resulting in the use of pattern 13[0-4]X because this stands for 10 possible numbers, while 13! stands for an unlimited amount of numbers.

Assume that the user dials 131. Then Cisco Unified Communications Manager would match the last three route patterns. After receiving these three digits and after the interdigit timer expires, only two patterns are left to match: 131 and 13!. Again, the more specific pattern, 131, is used to route the call.

Cisco Unified Communications Manager Digit Analysis

This topic describes how digit analysis is performed for different devices based on their addressing methods.

Cisco Unified Communications Manager Addressing Method		
Device	Signaling Protocol	Addressing Method
IP Phone	SCCP	Digit-by-digit
	SIP	En-bloc KPML SIP dial rules
		En-bloc
	MGCP/SIP/H.323	Overlap sending and receiving (ISDN PRI only)
Trunk	SIP, H.323	En-bloc Overlap sending and receiving

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-21

The table shows the supported addressing methods in Cisco Unified Communications Manager for different devices.

In SIP, en bloc dialing can be used, in which the whole dialed string is sent in a single SIP INVITE message, or KPML can be used which allows digits to be sent one-by-one. SIP dial rules are dial rules that are processed inside the SIP phone. Thus, a SIP phone can detect invalid numbers and play a reorder tone without sending any signaling messages to Cisco Unified Communications Manager. If dialed digits match an entry of a SIP dial rule, the dialed string is sent in a single INVITE message to Cisco Unified Communications Manager. If Cisco Unified Communications Manager requires more digits, KPML can be used to send the remaining digits from the SIP phone to Cisco Unified Communications Manager one-by-one.

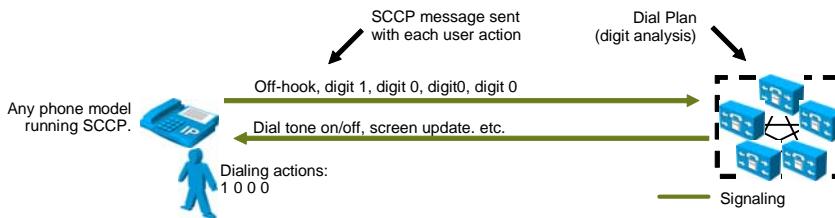
Trunks and ISDN PRIs can be configured for overlap sending and receiving, allowing digits to be sent or received one-by-one over an ISDN PRI.

User Input on SCCP Phones

This subtopic describes how user input on SCCP phones is handled by Cisco Unified Communications Manager.

User Input on SCCP Phones

- SCCP Phones report every input event (off-hook, on-hook, each digit dialed, etc.) to Unified CM immediately.
- Unified CM analyzes phone input digit-by-digit against configured dial plan and responds with feedback (dial tones, ring back, reorder tone, etc.).
- No dial plan information at the IP phone.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-22

IP phones using SCCP report every user input event to Cisco Unified Communications Manager immediately. For instance, as soon as the user goes off-hook, a signaling message is sent from the phone to the Cisco Unified Communications Manager server with which it is registered. The phone functions like a terminal, where all decisions resulting from user input are made by the configured dial plan of the Cisco Unified Communications Manager server.

As other user events are detected by the phone, they are relayed to Cisco Unified Communications Manager individually. A user who goes off-hook and then dials 1000 would trigger five individual signaling events from the phone to Cisco Unified Communications Manager. All the resulting feedback provided to the user, such as screen messages, playing dial tone, secondary dial tone, ring back, reorder, and so on, are commands issued by Cisco Unified Communications Manager to the phone in response to the dial plan configuration.

It is neither required nor possible to configure dial plan information on IP phones running SCCP. All dial plan functionality is contained in the Cisco Unified Communications Manager cluster, including the recognition of dialing patterns as user input is collected.

If the user dials a pattern that is denied by Cisco Unified Communications Manager, a reorder tone is played to the user as soon as that pattern becomes the best match in Cisco Unified Communications Manager digit analysis. For instance, if all calls to 91976 are denied, a reorder tone would be sent to the user phone as soon as the user dials 91976.

User Input on SIP Phones

Cisco Unified IP phones running SIP have different capabilities based on the IP phone model.

User Input on SIP Phones

- Type A SIP phones
 - Cisco Unified IP phones 7905, 7912, 7940, and 7960
 - Do not support KPML
- Type B SIP phones
 - Cisco Unified IP phones 7911, 7941, 7961, 7970, and 7971
 - Support KPML
- SIP dial rules can be configured on both phone types

© 2008 Cisco Systems, Inc. All rights reserved.

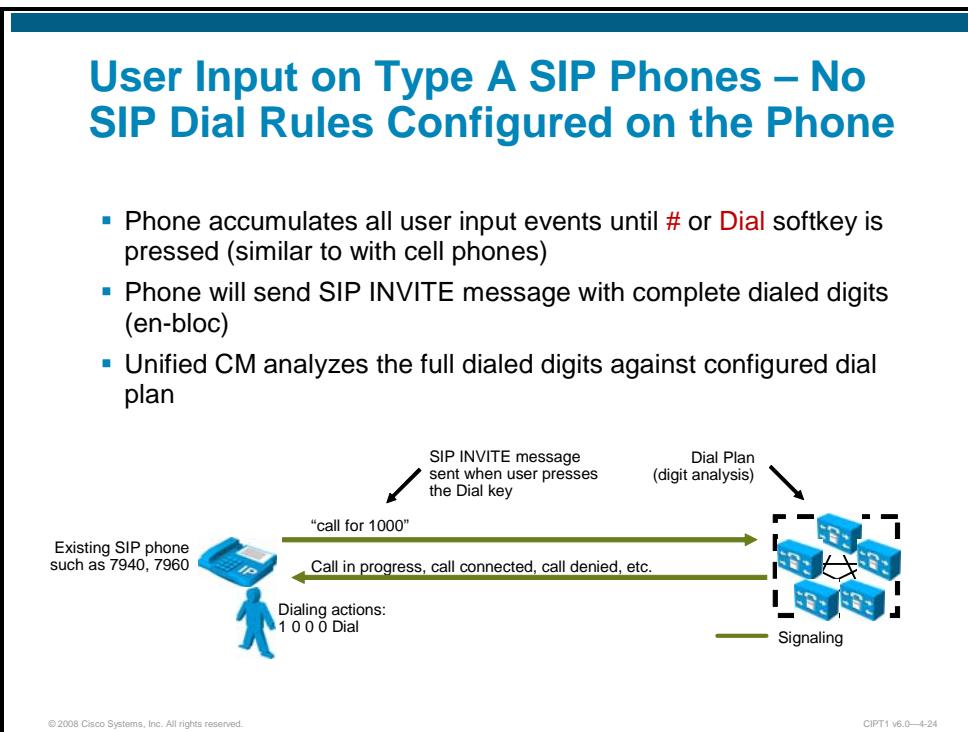
CIPT1 v6.0—4-23

Type A phones (Cisco Unified IP Phone 7905, 7912, 7940, and 7960) do not support KPML. They do support SIP dial rules, which are configured in Cisco Unified Communications Manager and downloaded to the IP phone at boot time.

Type B phones (Cisco Unified IP Phone 7911, 7941, 7961, 7970, and 7971) support KPML and SIP dial rules.

User Input on Type A SIP Phones – No SIP Dial Rules Configured on the Phone

The figure illustrates how user input is handled on type A SIP phones if no SIP dial rules are configured.

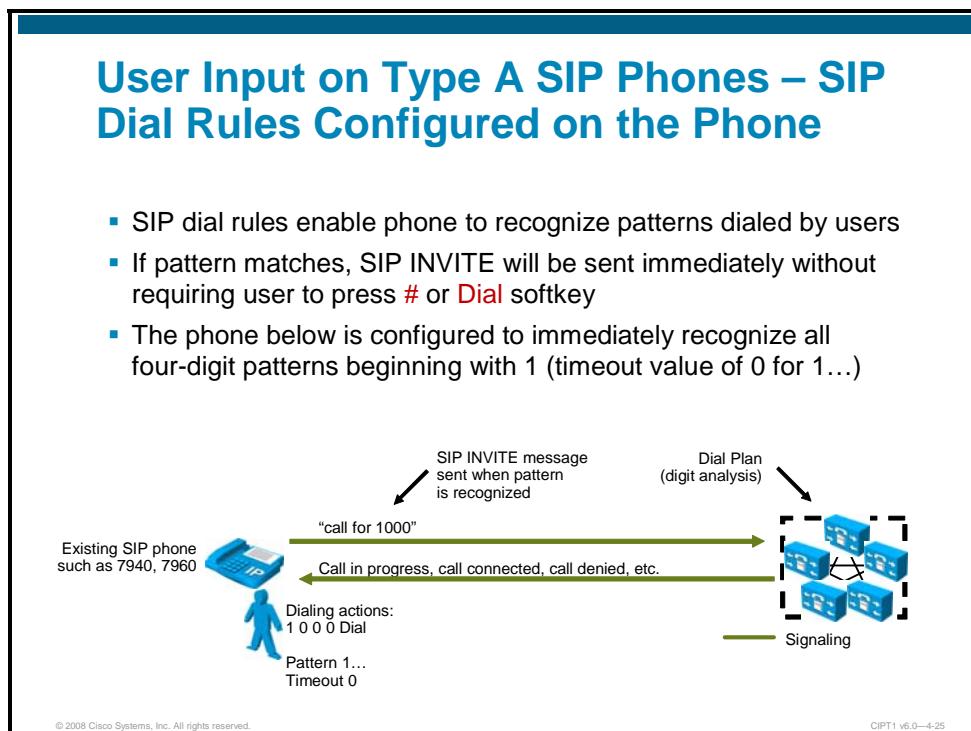


In this mode of operation, the phone accumulates all user input events until the user presses either the # key or the **Dial** softkey. This function is similar to the “send” button used on many mobile phones.

For example, a user making a call to extension 1000 would have to press 1, 0, 0, and 0 followed by the Dial softkey or the # key. The phone would then send a SIP INVITE message to Cisco Unified Communications Manager to indicate that a call to extension 1000 is requested. As the call reaches Cisco Unified Communications Manager, it is subjected to the dial plan configuration for this phone, including all the class-of-service and call-routing logic implemented in the Cisco Unified Communications Manager dial plan.

User Input on Type A SIP Phones – SIP Dial Rules Configured on the Phone

The figure illustrates how user input is handled on type A SIP phones if SIP dial rules are configured.



SIP dial rules enable the phone to recognize patterns dialed by users. Once the recognition has occurred, the sending of the SIP INVITE message to Cisco Unified Communications Manager is automated and does not require the user to press the Dial key or wait for the interdigit timeout.

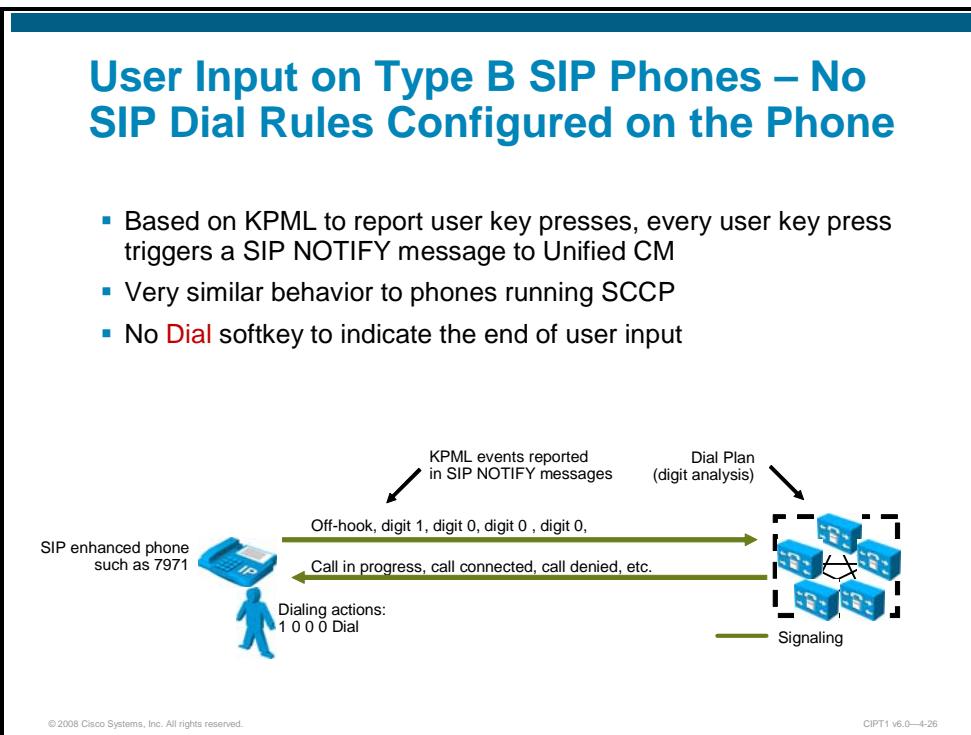
For example, if a branch location of the enterprise requires that calls between phones within the same branch be dialed as four-digit extensions, the phone could be configured to recognize the four-digit patterns so that the user is not required to press the Dial key or wait for the interdigit timeout. (See the diagram).

In the diagram in the figure, the phone is configured to recognize all four-digit patterns beginning with 1 and has an associated timeout value of 0. All user input actions matching the pattern will trigger the sending of the SIP INVITE message to Cisco Unified Communications Manager immediately, without requiring the user to press the Dial key. Type A phones using SIP dial rules offer a way to dial patterns not explicitly configured on the phone. If a dialed pattern does not match a SIP dial rule, the user can press the Dial key or wait for interdigit timeout.

If a particular pattern is recognized by the phone but blocked by Cisco Unified Communications Manager, the user must dial the entire dial string before receiving an indication that the call is rejected by the system. For instance, if a SIP dial rule is configured on the phone to recognize calls dialed in the form 919765551234 but such calls are blocked by the Cisco Unified Communications Manager dial plan, the user will receive a reorder tone at the end of dialing (after pressing the final 4 key).

User Input on Type B SIP Phones – No SIP Dial Rules Configured on the Phone

The figure illustrates how user input is handled on type B SIP phones if no SIP dial rules are configured.



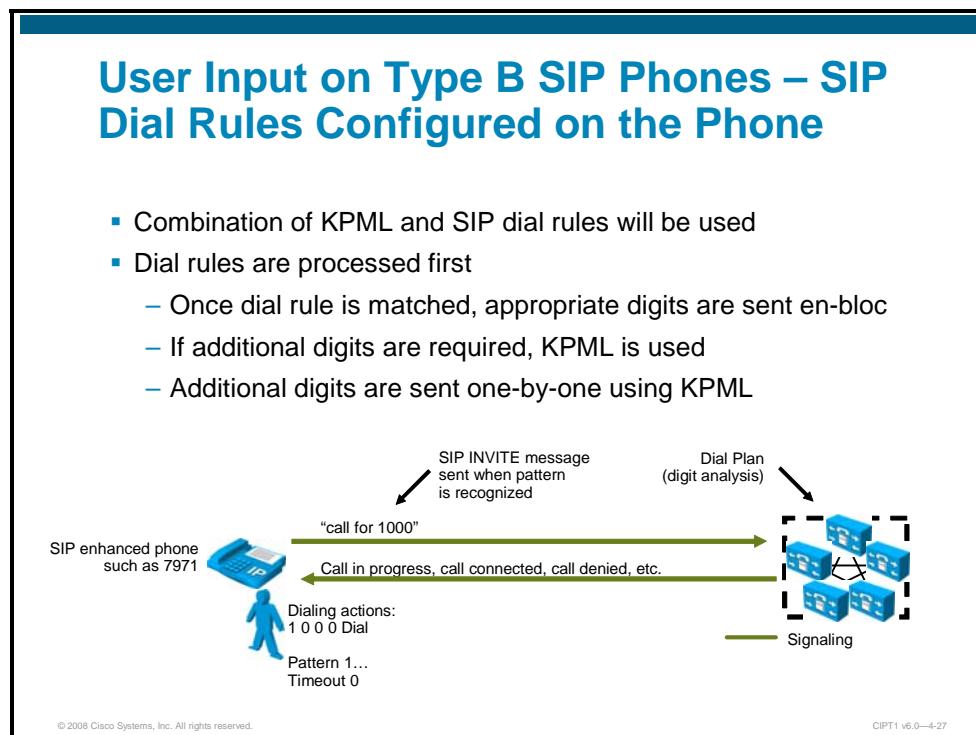
Type B IP phones offer functionality based on the KPML to report user activities. Each one of the user input events generates its own KPML-based message to Cisco Unified Communications Manager. From the standpoint of relaying each user action immediately to Cisco Unified Communications Manager, this mode of operation is similar to that of phones running SCCP.

Every user key press triggers a SIP NOTIFY message to Cisco Unified Communications Manager to report a KPML event corresponding to the key pressed by the user. This messaging enables Cisco Unified Communications Manager digit analysis to recognize partial patterns as they are composed by the user, and to provide appropriate feedback, such as immediate reorder tone if an invalid number is being dialed.

In contrast to Type A IP phones running SIP without dial rules, Type B SIP phones have no Dial key to indicate the end of user input. In the diagram, a user dialing 1000 would be provided call progress indication (either ringback tone or reorder tone) after dialing the last 0 and without having to press the Dial key. This behavior is consistent with the user interface on phones running the SCCP protocol.

User Input on Type B SIP Phones – SIP Dial Rules Configured on the Phone

The figure illustrates how user input is handled on type B SIP phones if SIP dial rules are configured.



Type B IP phones can be configured with SIP dial rules so that dialed pattern recognition is accomplished by the phone. In the figure, the phone is configured to recognize all four-digit patterns beginning with 1, and it has an associated timeout value of 0. All user input actions matching these criteria will trigger the sending of a SIP INVITE message to Cisco Unified Communications Manager.

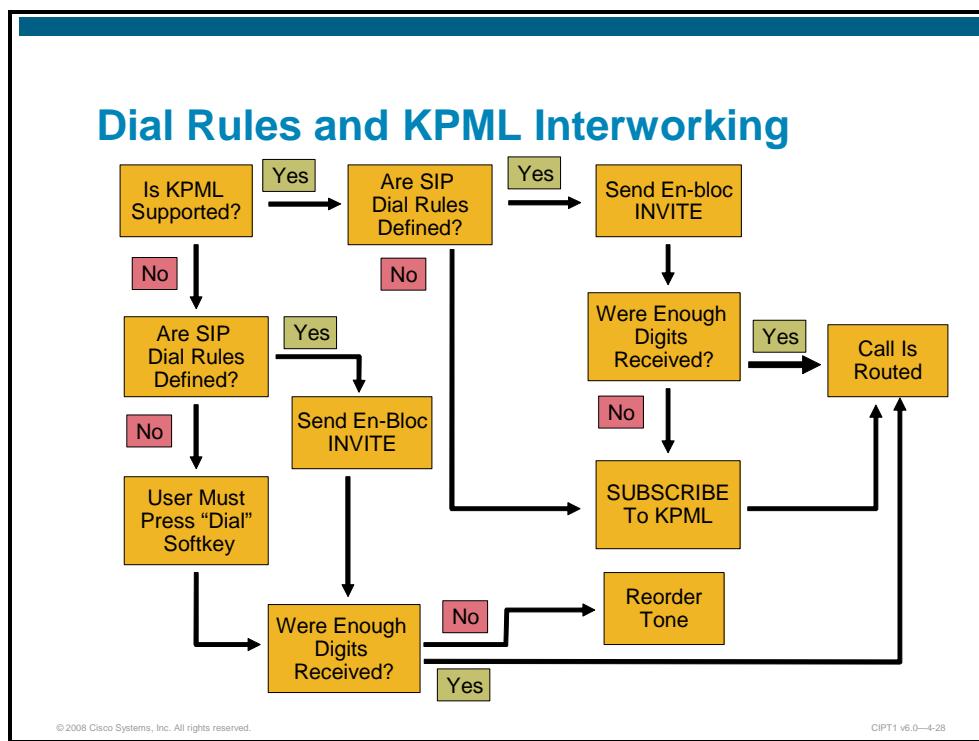
As soon as SIP dial rules are implemented on Type B IP phones, KPML-based dialing is used if the dial string, which matched a dial rule and was passed on to Cisco Unified Communications Manager in the SIP INVITE message, requires more digits at Cisco Unified Communications Manager (because there are potential matches which are longer than the provided dial string).

Type B phones using SIP dial rules offer only one way to dial patterns not explicitly configured on the phone. If a dialed pattern does not match a SIP dial rule, the user has to wait for interdigit timeout before the SIP NOTIFY message is sent to Cisco Unified Communications Manager. Unlike type A IP phones, type B IP phones do not have a Dial key to indicate the end of dialing, except when on-hook dialing is used. In the latter case, the user can press the Dial key at any time to trigger the sending of all dialed digits to Cisco Unified Communications Manager.

If a particular pattern is recognized by the phone but blocked by Cisco Unified Communications Manager, the user must dial the entire dial string before receiving an indication that the call is rejected by the system. For instance, if a SIP dial rule is configured on the phone to recognize calls dialed in the form 919765551234, but such calls are blocked by the Cisco Unified Communications Manager dial plan, the user will receive a reorder tone at the end of dialing (after pressing the 4 key).

Dial Rules and KPML Interworking

The figure shows the interworking of dial rules and KPML on Cisco type B SIP IP phones.



If KPML is supported and SIP dial rules are configured, digits are sent en bloc in a SIP INVITE message after matching a dial rule. If Cisco Unified Communications Manager requires additional digits for the call routing decision, KPML is used to transfer the additional digits. If no additional digits are provided, Cisco Unified Communications Manager stops digit collection after expiration of the interdigit timer and rejects the call.

Gateway Overlap Sending and Receiving

This subtopic describes overlap sending and receiving, which can be enabled on ISDN PRIs.

Gateway Overlap Sending and Receiving

Overlap Sending

- Unified CM collects digits and immediately passes them on to the PSTN one-by-one as they are dialed.
- Very useful for simplifying variable-length PSTN dial patterns (just need a single route pattern for all PSTN calls).
- Configured through route pattern configuration.

Overlap Receiving

- Unified CM receives the dialed digits one-by-one from a PRI PSTN gateway.
- Configured globally through Unified CM service parameter.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-29

In countries whose national numbering plan is not easily defined with static route patterns, Cisco Unified Communications Manager can be configured for overlap sending and overlap receiving. Overlap sending means that Cisco Unified Communications Manager keeps collecting digits as they are dialed by the end users, and passes them on to the PSTN as they are dialed. To enable overlap sending, check the **Allow Overlap Sending** box on the Route Pattern configuration page. The route pattern needs only to include the PSTN access code (for example, "9." in North America or "0." in many European countries).

Overlap receiving means that Cisco Unified Communications Manager receives the dialed digits one-by-one from a PRI PSTN gateway, and it waits for completion of the dialed string before attempting to route the call to an internal destination. To enable overlap receiving, set the **OverlapReceivingFlagForPRI** service parameter to True.

Cisco Unified Communications Manager Path Selection

This topic describes path selection in Cisco Unified Communications Manager.

Path Selection

- Path selection is an essential dial plan element.
- After call routing decision is done, where should the call be sent to?
- Chooses the best path:
 - Which device to use (gateways, trunks, etc.)?
 - Backup path available if first choice not available?

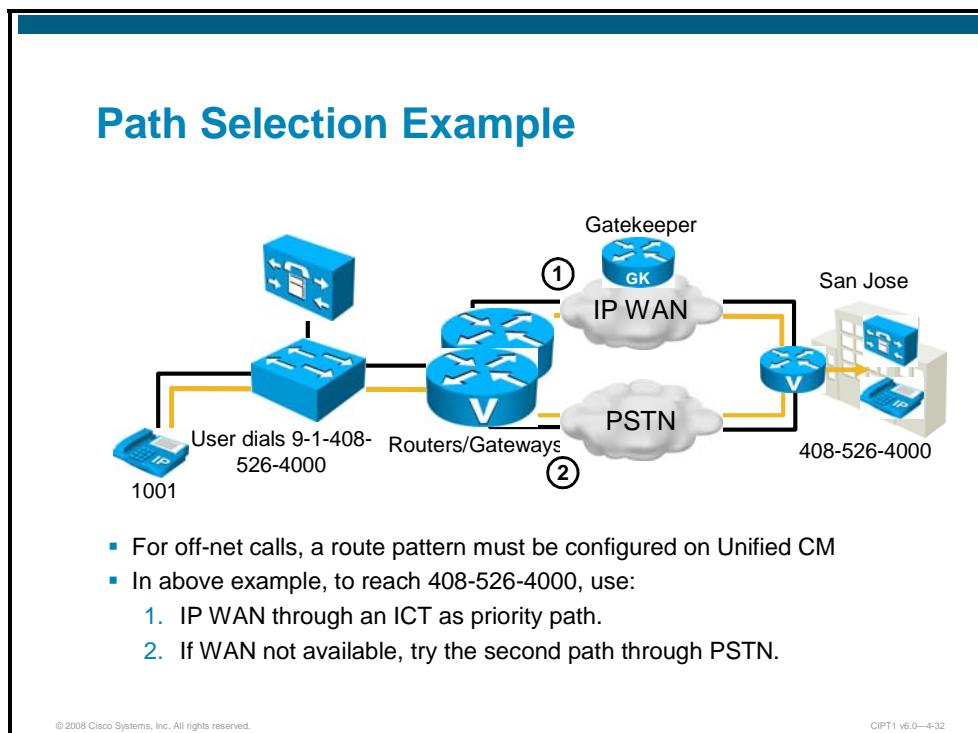
© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-31

Path selection is an essential dial plan element. After matching an entry in the call routing table, Cisco Unified Communications Manager has to select how to route the call and where to route the call to. The routing might be a VoIP path over an IP network using a Cisco Unified Communications Manager trunk or a path using the PSTN. Cisco Unified Communications Manager allows multiple paths to be configured for a route pattern in order to specify a primary path and one or more backup paths.

Path Selection Example

The figure shows two possible paths to be used for a dialed route pattern.



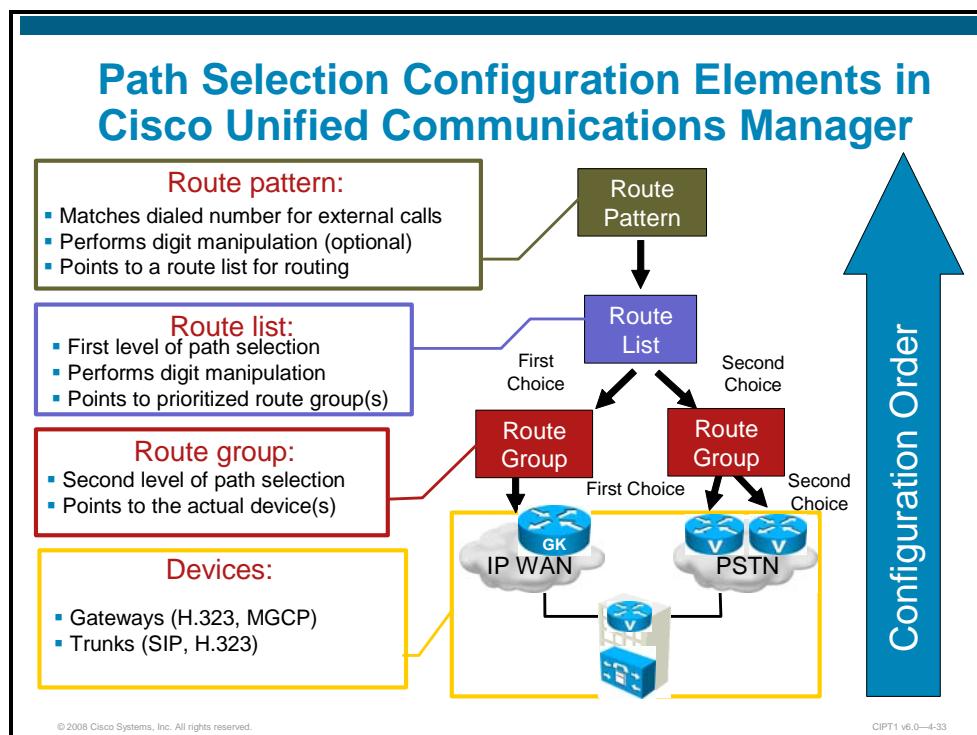
In the figure, if a user dials a long-distance PSTN number such as 9-1-408-526-4000, the call should be sent over the IP WAN, such as over a gatekeeper-controlled H.323 intercluster trunk. If this path does not work (network failure, no response from the other side, and so on) the call should use the local PSTN gateway as a backup and send the call through the PSTN.

For such off-net calls, route patterns must be configured in Cisco Unified Communications Manager. Assuming that the office in San Jose has a direct inward dial range of 4000–4999, the route pattern would be 9.14085264XXX, where the 9 is used as a PSTN access code, the 1 is used to indicate a long-distance call, 408 is the area code, 526 is the office code, and 4XXX stands for station codes 4000 to 4999.

Note	Usually, digit manipulation must be performed depending on the selected path. In the example, for the PSTN call, the access code 9 has to be removed and the calling party number should be changed from the internal extension 1001 to a full PSTN number. If the call is sent over the IP WAN, a different dial string than the PSTN number might be used to address the destination.
-------------	---

Path Selection Configuration Elements in Cisco Unified Communications Manager

The figure shows the configuration elements that are used to select the path for a given route pattern.



Route patterns are strings of digits and wildcards, such as 9.4085264XXX, configured in Cisco Unified Communications Manager and part of the call routing table. If matched by the call routing logic, the route pattern can point directly to a device such as a trunk or a gateway, or point to a route list. Route lists provide the first level of path selection, if multiple paths exist to reach the called number that matches the route pattern. Route lists include a prioritized list of route groups and allow digit manipulation to be configured per route group. A route group is the second level of path selection. It points to devices which are selected based on a distribution algorithm (circular or top down).

Cisco strongly recommends using the complete route pattern, route list, and route group construct because it provides the greatest flexibility for call routing, digit manipulation, route redundancy, and future dial plan growth. If route patterns point directly to devices, the configuration might need to be changed later when additional devices are added. A single device cannot be used in both ways, being a member in a route group and being referenced directly from a route pattern.

Cisco Unified Communications Manager Path Selection Configuration

This topic describes how to configure path selection in Cisco Unified Communications Manager.

Path Selection Configuration Process

1. Add devices (gateways and trunks).
2. Build route groups from available devices.
3. Build route lists from available route groups.
4. Build route patterns pointing to route lists.

© 2008 Cisco Systems, Inc. All rights reserved.

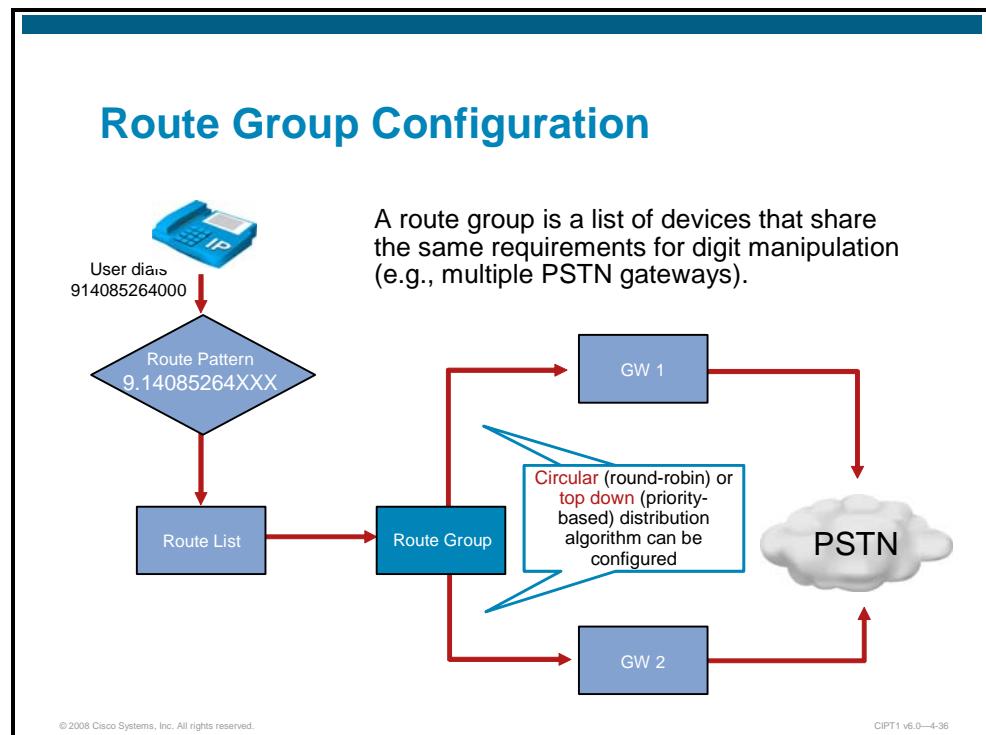
CIPT1 v6.0—4-35

To implement path selection in Cisco Unified Communications Manager, follow these high-level steps in the given order:

- Step 1** Add devices (gateways and trunks).
Step 2 Build route groups from available devices.
Step 3 Build route lists from available route groups.
Step 4 Build route patterns pointing to route lists.

Route Group Configuration

This subtopic provides more information about route group configuration.



A route group is a list of devices (gateways and trunks). It is recommended to put such devices into the same route group that has identical digit manipulation requirements, because then digit manipulation can be configured once per route group during route list configuration.

Note	A route group can be configured for circular distribution (round robin) or for top-down distribution (first entry of list has highest priority). The circular distribution is used for load-sharing scenarios while the top-down distribution is used to implement backup paths in case the preferred path is not available.
-------------	--

Route Group Configuration

The screenshot shows an example of route group configuration.

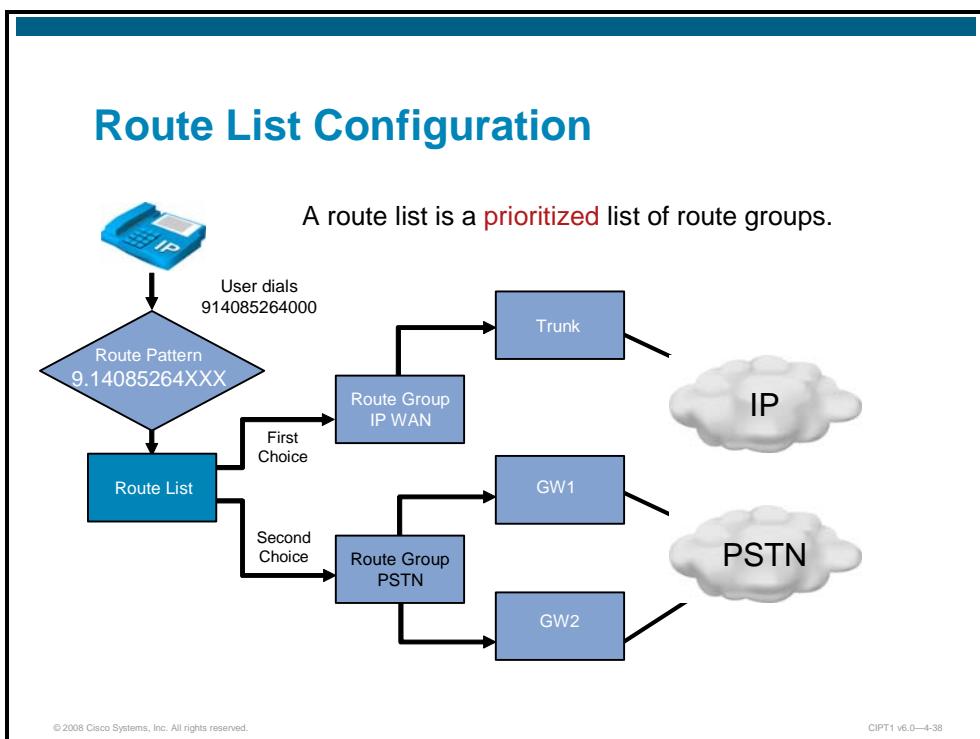
The screenshot displays the 'Route Group Configuration' page. At the top, there's a header bar with the title 'Route Group Configuration'. Below it, the main form is divided into several sections:

- Route Group Information:** Contains fields for 'Route Group Name' (set to 'PSTN') and 'Distribution Algorithm' (set to 'Circular'). A callout box labeled 'Select distribution algorithm' points to this section.
- Route Group Member Information:** Includes a 'Find Devices to Add to Route Group' section with a 'Device Name contains' field and a 'Find' button. Below it is a list of 'Available Devices' (GW1, GW2, S0/SU3/DS1-0@HQ-1) and a dropdown for 'Port(s)' set to 'All'. A blue arrow points from this section to a callout box labeled 'Add gateways and trunks to route group', which points to the 'Add to Route Group' button.
- Current Route Group Members:** Shows a list of 'Selected Devices' (GW1 (All Ports), GW2 (All Ports)) with a red-bordered 'Reverse Order of Selected Devices' button. Another blue arrow points from this section to the same 'Add to Route Group' button.
- Buttons:** At the bottom left is a 'Save' button, and at the bottom right is a copyright notice: '© 2008 Cisco Systems, Inc. All rights reserved.' and 'CIPT1 v6.0—4-37'.

In the example, two devices (GW1 and GW2) have been put into the route group. The distribution algorithm is circular, therefore the order of the gateways is not important.

Route List Configuration

This subtopic provides more information about route list configuration.



A route list is a list of prioritized route groups. When configuring a route list, you can set up digit manipulation per route group within the route list.

Route List Configuration Example

The screenshot shows an example of route list configuration.

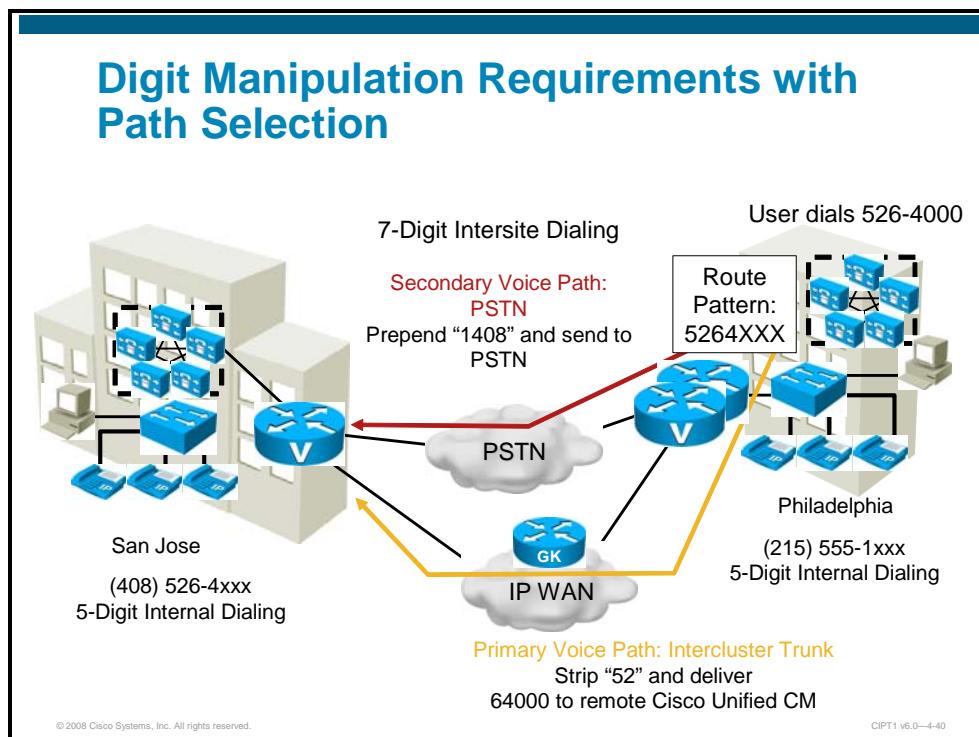
The screenshot displays the 'Route List Configuration' page. At the top, the title 'Route List Configuration' is shown in blue. Below it, the 'Route List Information' section includes fields for 'Name*' (San Jose Office), 'Description', 'Cisco Unified Communications Manager Group*' (Default), and a checked checkbox for enabling the route list. The 'Route List Member Information' section contains two lists: 'Selected Groups**' (WAN, PSTN) and 'Removed Groups***'. An 'Add Route Group' button is located between these lists. A callout box points to this button with the text 'Add route groups to route list'. The 'Route List Details' section at the bottom shows route group icons for PSTN and WAN, with the WAN icon highlighted. A callout box points to this section with the text 'Order route list members (first entry has highest priority)'. At the very bottom, there are buttons for Save, Delete, Copy, Reset, and Add New.

In the example, two route groups have been added to the route list. Route group WAN is listed first and therefore has highest priority. If calls cannot be set up using any device of the WAN route group, the next route group (PSTN) is used. Again, Cisco Unified Communications Manager tries all devices of that route group according to the route group distribution algorithm (circular or top-down). A route list can be disabled, which means that it remains in the configuration database but will not be used.

At the bottom of the route list configuration page, in the Route List Details field, you can configure route list details per route group. This is where you can configure digit manipulation for each route group that is a member of the route list.

Digit Manipulation Requirements with Path Selection

The figure illustrates digit manipulation requirements when different paths can be taken for a call.



In this example, there are two sites, San Jose and Philadelphia. Each phone has a corresponding PSTN DID number. Users dial five-digit extensions within a site (the last digit of the PSTN office code plus the DID subscriber numbers). For intersite calls, users dial seven digits (the PSTN office code used at each site plus the DID subscriber number).

At the Cisco Unified Communications Manager in Philadelphia, a route pattern 5264XXX is configured for intersite calls toward San Jose. The route pattern points to a route list with two route groups. One route group refers to an intercluster trunk (configured as the primary path), and the other route group refers to a group of PSTN gateways (as a backup path). Depending on the chosen path, the following digit manipulation requirements apply for a call placed from Philadelphia to 526-4000:

- **Calls routed over the intercluster trunk:** The first two digits (52) of the called number (526-4000) have to be stripped so that the receiving Cisco Unified Communications Manager in San Jose finds the five-digit number as a configured directory number on one of its IP phones. In addition, the calling party number has to be changed from a five-digit extension to a seven-digit intersite route pattern (by prefixing 55).
- **Calls routed over the PSTN:** The called number has to be extended to a full PSTN number by prepending 1408 to the dialed seven-digit number. At the receiving side, incoming calls from the PSTN have to be changed to five-digit internal directory numbers. The calling number has to be changed to a full PSTN number.

Note	More information about digit manipulation configuration is provided in another lesson of this module.
-------------	---

Special Call Routing Features

This topic describes special call routing features that can be used in Cisco Unified Communications Manager.

The @ Wildcard

- Macro function that expands into a series of route patterns
- Represents the entire national numbering plan for a certain country
- Example, configuring a 9.@ route pattern adds 166 individual NANP route patterns to Unified CM database
- It is possible to modify and use @ for other country numbering plan
- Can be used with route filters to block certain components of the number

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-42

The @ wildcard is a special macro function that expands into a series of patterns representing the entire national numbering plan for a certain country. For example, configuring a single unfiltered route pattern such as 9.@ with the North American Numbering Plan (NANP) adds 166 individual route patterns to the Cisco Unified Communications Manager internal dial plan database.

It is possible to configure Cisco Unified Communications Manager to accept other national numbering plans. Once this is done, the @ wildcard can be used for different numbering plans, even within the same Cisco Unified Communications Manager cluster, depending on the value selected in the Numbering Plan field on the Route Pattern configuration page.

The @ wildcard can be practical in small and medium deployments, but it can become harder to manage and troubleshoot in large deployments. Certain components of the numbering plan can be matched by the use of route filters.

Route Filters

This subtopic describes how route filters work together with numbering plans in Cisco Unified Communications Manager.

Route Filters

- Used only with @ route pattern to block certain patterns (e.g., block all 1-900 calls, etc.) defined by clauses
- Not recommended for large deployments; use explicit route patterns rather than @ wildcard
- Match clauses are based on tag operators and values
- Example, Match all NANP dialed numbers that include area code 408 (e.g., 9.14085551234)
 - Route pattern: 9.@
 - Route filter: IF AREA-CODE = 408
- Example: Match all NANP dialed numbers that include the selection of a long-distance carrier (e.g., 9.101044414085551234)
 - Route pattern: 9.@
 - Route filter: IF TRANSIT-NETWORK EXISTS

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-43

Route filters can only be used with the @ route pattern to match certain elements or special numbers of a numbering plan. A route filter applied to a pattern not containing the @ wildcard is ignored.

The logical expression entered with the route filter can be up to 1024 characters, excluding the NOT-SELECTED fields.

For large-scale deployments, use explicit route patterns rather than the @ wildcard and route filters. This practice also facilitates management and troubleshooting because all patterns configured in Cisco Unified Communications Manager are easily visible from the Route Pattern configuration page.

Tags serve as the core component of a route filter. A tag applies a name to a subset of the dialed-digit string. For example, the NANP number 972-555-1234 comprises LOCAL-AREA-CODE (972), OFFICE-CODE (555), and SUBSCRIBER (1234) route filter tags. The complete list of tags available for the NANP is shown in the following table:

Tag	Description
AREA-CODE	This three-digit area code in the form [2–9]XX identifies the area code for long-distance calls.
COUNTRY CODE	These one-, two-, or three-digit codes specify the destination country for international calls.
END-OF-DIALING	This single character identifies the end of the dialed-digit string. The # character serves as the end-of-dialing signal for international numbers that are dialed within the NANP.
INTERNATIONAL-ACCESS	This two-digit access code specifies international dialing. Calls that originate in the U.S. use 01 for this code.
INTERNATIONAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed international call. Calls that originate in the U.S. use 1 for this code.
INTERNATIONAL-OPERATOR	This one-digit code identifies an operator-assisted international call. This code specifies 0 for calls that originate in the U.S.
LOCAL-AREA-CODE	This three-digit local area code in the form [2–9]XX identifies the local area code for 10-digit local calls.
LOCAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed local call. NANP calls use 1 for this code.
LOCAL-OPERATOR	This one-digit code identifies an operator-assisted local call. NANP calls use 0 for this code.
LONG-DISTANCE-DIRECT-DIAL	This one-digit code identifies a direct-dialed, long-distance call. NANP calls use 1 for this code.
LONG-DISTANCE-OPERATOR	These one- or two-digit codes identify an operator-assisted, long-distance call within the NANP. Operator-assisted calls use 0 for this code, and operator access uses 00.
NATIONAL-NUMBER	This tag specifies the nation-specific part of the digit string for an international call.
OFFICE-CODE	This tag designates the first three digits of a seven-digit directory number in the form [2–9]XX.
SATELLITE-SERVICE	This one-digit code provides access to satellite connections for international calls.
SERVICE	This three-digit code designates services such as 911 for emergency, 611 for repair, and 411 for information.
SUBSCRIBER	This tag specifies the last four digits of a seven-digit directory number in the form XXXX.
TRANSIT-NETWORK	This four-digit value identifies a long-distance carrier. Do not include the leading 101 carrier access code prefix in the TRANSIT-NETWORK value. Refer to TRANSIT-NETWORK-ESCAPE for more information.
TRANSIT-NETWORK-ESCAPE	This three-digit value precedes the long-distance carrier identifier. The value for this field specifies 101. Do not include the four-digit carrier identification code in the TRANSIT-NETWORK-ESCAPE value. Refer to TRANSIT-NETWORK for more information.

Examples of route filters:

- **Example 1:** A route filter that uses AREA-CODE and the operator DOES-NOT-EXIST selects all dialed-digit strings that do not include an area code (for example, seven-digit calls).
- **Example 2:** A route filter that uses AREA-CODE, the operator ==, and the entry 515 selects all dialed-digit strings that include the 515 area code (equivalent to a route pattern 515XXXXXXX or 1515XXXXXXX).
- **Example 3:** A route filter that uses AREA-CODE, the operator ==, and the entry 5[2-9]X selects all dialed-digit strings that include area codes in the range of 520 through 599.
- **Example 4:** A route filter that uses TRANSIT-NETWORK, the operator ==, and the entry 0444 selects all dialed-digit strings with the carrier access code 1010444.

The ! Wildcard

This subtopic describes the ! wildcard that can be used in route patterns.

The ! Wildcard

- Stands for one or more digits
- Used for variable-length route patterns (e.g., some international calls)
- Subject to T302 timer (post-dial delay)
 - 15 seconds by default
 - T302 timer can be configured (typically reduced):
 - **Service Parameter > Call Manager > Clusterwide parameters (Device – General)**
- Users can indicate end of dialing by pressing #
 - Requires an identical route pattern with # wildcard at the end
 - Different behavior compared to Cisco IOS dial peers
 - In Unified CM, # is seen as part of dialed string (therefore, if used, it does not match route pattern without #)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-44

International destinations are usually configured using the ! wildcard, which represents any quantity of digits. For example, in North America the route pattern 9.011! is typically configured for international calls. In most European countries, the same result is accomplished with the 0.00! route pattern.

The ! wildcard is also used for deployments in countries where the dialed numbers can be of varying lengths. In such cases, Cisco Unified Communications Manager does not know when the dialing is complete and will wait for 15 seconds (by default) before sending the call. This delay can be reduced in any of the following ways:

- Reduce the T302 timer (Service Parameter TimerT302_msec) to indicate end of dialing, but do not set it lower than 4 seconds to prevent premature transmission of the call before the user is finished dialing.
- Configure a second route pattern followed by the # wildcard (for example, 9.011#! for North America or 0.00#!# for Europe), and instruct the users to dial # to indicate end of dialing. This action is analogous to hitting the “send” button on a cell phone.

Note	Regarding the # wildcard, note that the implementation of the interdigit timeout termination is different than the implementation in Cisco IOS dial peers. In Cisco Unified Communications Manager, the # is not only the instruction to stop digit collection but it is part of the dialed number. Therefore, if users are to choose whether or not to use the # in order to prevent waiting for the expiration of the interdigit timeout, all route patterns have to be configured twice, once with the # and once without it.
-------------	--

Urgent Priority

This section describes what urgent priority is, where it can be configured, and how it works.

Urgent Priority

- Configured under Route Pattern configuration
- Used to force immediate routing as soon as match is detected – even if other, longer route patterns are potential matches
- Used with emergency number route patterns
- Effectively excludes the urgent pattern from a longer route pattern range
- Translation patterns always have urgent priority

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-45

The Urgent Priority checkbox is often used to force immediate routing of certain calls as soon as a match is detected, without waiting for the T302 timer to expire when additional longer potential matches exist. For example, in North America, if the patterns 9.911 and 9.[2-9]XXXXXX are configured and a user dials 9911, Cisco Unified Communications Manager usually has to wait for the T302 timer before routing the call, because further digits may cause the 9.[2-9]XXXXXX to match. If Urgent Priority is enabled for the 9.911 route pattern, Cisco Unified Communications Manager makes its routing decision as soon as the user has finished dialing 9911, without waiting for the T302 timer. Effectively, urgent priority excludes the route pattern where it has been enabled from other, longer route patterns.

If en bloc dialing is used and the provided number is longer than the urgent pattern, the urgent pattern is not considered.

Translation patterns always have urgent priority enabled (and it cannot be disabled).

Blocked Patterns

The subtopic describes the parameter Block This Pattern.

Blocked Patterns

- A route pattern can be configured for either “Allow” or “Block”.
- Block patterns will prevent calls to the pattern cluster-wide.
- The same can be configured on translation patterns.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-46

Route patterns and translation patterns can be configured to block the pattern. Patterns that are blocked prevent calls to the blocked pattern cluster-wide.

Note	If certain destinations should be blocked, depending on the calling device or user, calling privileges have to be configured. With calling privileges, individual classes of service can be configured per calling device. Blocked patterns, on the other hand, generally do not allow calls to the matched number.
-------------	---

Call Classification

This subtopic describes call classification in Cisco Unified Communications Manager.

Call Classification

- Classify a call as on-net or off-net
- Configured on route patterns for outgoing calls and devices (trunks and gateways) for incoming calls
- “Allow device override” setting uses the classification of the used device on outgoing calls (rather than route pattern classification)
- Used by several features:
 - Blocking off-net to off-net transfers (toll-fraud prevention)
 - Drop conference when no on-net party remains
 - Call forward external versus call forward internal

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-47

Route patterns and devices can be classified as on-net or off-net.

The configuration at route patterns is used for outgoing calls, while the setting at the device is used for incoming calls.

At the route pattern, the Allow Device Override parameter can be activated, which changes the default classification method for outgoing calls. Rather than the route patterns classification, the classification of the outgoing device is used. This is useful, when the route pattern refers to a route list with multiple options for path selection. Assume that the first path is an intercluster trunk, which should be considered to be an on-net call because it uses the IP network, and the second path is using a PSTN gateway, which should be considered to be an off-net call. This distinction is not possible if the route patterns classification is used.

The classification is used by several features, including the following:

- **Call Forward settings:** Call forward can be configured differently for internal (on-net) versus external (off-net) calls.
- **Block off-net to off-net transfers:** This is a toll fraud prevention feature that ensures that the company telephony infrastructure is not misused to connect two external parties (usually separated by a long distance) by an internal facilitator.
- **Drop conference when no on-net party remains:** This is a toll-fraud prevention feature that ensures that a conference is dropped when only external parties remain in the conference. If the setting is not enabled, an internal facilitator could again try to connect two external parties, this time by setting up a conference and then dropping out, leaving the two external parties alone in the conference.

Note	Call forwarding is enabled at the phone; the other two features are Cisco Unified Communications Manager service parameters.
-------------	--

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- A uniform on-net dial plan provides unique endpoint addressing by fixed-length directory numbers.
- Call routing is when Unified CM processes incoming call requests by looking up the dialed number in its call routing table.
- Unified CM can receive dialed digits one-by-one or en bloc.
- Unified CM allows multiple, prioritized paths to be selected for a given route pattern.
- Route lists, route groups, and devices are configured to implement path selection.
- Unified CM configuration includes special call routing features such as numbering plans and route filters, a wildcard for variable length numbers, blocked patterns, patterns with urgent priority, and classification of calls.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-48

References

For additional information, refer to these resources:

- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Cisco Unified Communications Manager Dial Plan Deployment Guide
http://www.cisco.com/en/US/products/sw/voicesw/ps5629/prod_maintenance_guides_list.html

Lesson 3

Implementing Cisco Unified Communications Manager Digit Manipulation

Overview

Users of a phone system often need to reach a variety of destinations, such as extensions located within the same site, different sites within the same company (sometimes with different dialing plans), and other companies located within the same country or different countries.

Because these calls can take different paths, such as the IP WAN or a preferred public switched telephone network (PSTN) carrier, completing these calls often requires dialing various access codes, numbers of digits, or prefixes. In addition, it is often prudent to restrict certain destinations, such as 900 numbers.

To require users to understand the specific dialing patterns necessary to reach these various destinations is impractical and inconvenient. Digit manipulation, or the ability of Cisco Unified Communications Manager to add or subtract digits to comply with a specific internal dial plan or national numbering plan, is the key to providing transparent dialing and creating a unified dialing plan for end users.

This lesson describes digit manipulation tools that allow a Cisco Unified Communications Manager Administrator to implement flexible and transparent dial plans. It describes external phone number mask, digit prefix and stripping, transformation masks, translation patterns, and significant digits.

Objectives

Upon completing this lesson, you will be able to use digit manipulation techniques to perform tasks such as expanding a calling-party directory number to a full E.164 PSTN number for outgoing PSTN calls, stripping a PSTN access code before sending a call to PSTN, expanding or modifying an abbreviated number to reach the actual destination (such as “0” for operator), converting an E.164 PSTN called-party directory number to an internal number for incoming calls from PSTN, and handling overlapping endpoint directory number issues. This ability includes being able to meet these objectives:

- Describe when to use digit manipulation in Cisco Unified Communications Manager
- Describe Cisco Unified Communications Manager digit manipulation operation
- List Cisco Unified Communications Manager digit manipulation configuration options
- Describe how to use external phone number masks
- Describe how to prefix and strip digits to and from called and calling party numbers
- Describe how to use translation patterns
- Describe how to use transformation masks in Cisco Unified Communications Manager
- Describe how to use digit stripping in Cisco Unified Communications Manager
- Describe how to use significant digits in Cisco Unified Communications Manager

Essentials of Cisco Unified Communications Manager Digit Manipulation

This topic describes Cisco Unified Communications Manager digit manipulation.

Digit Manipulation

The diagram shows a network architecture for off-net calls. On the left, a yellow box represents the internal network containing Cisco IP Phones (extension 1002), SIP 3rd party IP Phone, CCM1-1, CCM2-1, and Local Gateways. An arrow points from extension 1002 to a blue box labeled 'Off-Net Calls'. This box contains a table:

	On-Net	Off-Net
Calling	1002	706-555-1002
Called	9.1408-555-1111	1408-555-1111

To the right, a blue cloud represents the PSTN. An arrow points from the Off-Net Calls box to the PSTN. A call flow box indicates 'DID: 706-555-1001 to 1003' and shows the number '408-555-1111' being dialed. To the right of the PSTN is a section titled 'How to Manipulate Calling and Called Number?' with two bullet points:

- Expand calling directory number to fully qualified PSTN number
- Strip access code 9 dialed internally for PSTN access

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-4

In some cases, it is required to manipulate the calling and called (dialed) string before routing a call; for example, when calling a PSTN number from an internal network, and the access code “9” must be stripped from the called number before sending it out to the PSTN. The calling party number must also be changed from a four-digit extension to a full E.164 PSTN number.

In the example in the figure, an IP phone with extension 1002 calls PSTN phone 408555111 by first dialing the PSTN access code “9” followed by the PSTN number. It is very important to strip 9 from the called number before sending the call to PSTN, or the PSTN switch will not be able to route the call to the correct destination. In addition the calling-party number must be expanded to a full PSTN number, so that when the PSTN phone rings, it sees the call coming from PSTN number 7065551002, and not from extension 1002. This will allow the PSTN phone to call back the number conveniently from its Received/Missed Calls menu.

Note	In some countries, the calling party number must be set to the correct PSTN number of the PSTN subscriber line or trunk.
-------------	--

Digit Manipulation Requirements

This topic describes some examples of digit manipulation requirements.

Digit Manipulation Requirements		
Requirement	Call Type	How
Expand calling-party directory number to full E.164 PSTN number	Internal to PSTN	Use calling party's external phone number mask or calling party transformation in route pattern or route list
Strip PSTN access code "9"	Internal to PSTN	Use Digit Stripping in Route Pattern or Route List
Expand abbreviated number (e.g., "0" for operator)	Internal to Internal	Use Called Party Transformation in Translation Pattern
Convert E.164 PSTN called-party directory number to internal number	PSTN to Internal	Use Called Party Transformation in Translation Pattern, or use Significant Digits
Overlapping endpoint directory number	Internal to Internal PSTN to Internal	Use Called Party Transformation in Translation Pattern

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-5

The table in the figure shows some examples of digit manipulation requirements and what tools you can use to implement them in Cisco Unified Communications Manager, as follows:

- To expand a calling-party directory number to a full E.164 PSTN number for outgoing PSTN calls, use either the external phone number mask or the calling party transformation mask of the calling party in the PSTN route pattern or route list.
- To strip a PSTN access code before sending the call to the PSTN, use digit stripping (discard digits instruction [DDI]) in the PSTN route pattern or route list.
- To expand or modify an abbreviated number to reach the actual destination (such as when access code "0" for operator must be converted to the actual internal extension of the operator), create a translation pattern and use the called party transformation mask to convert the number. This is also applicable for calls to on-net sites, where you must use the private IP WAN as much as possible, even though the user calls the PSTN number to reach those sites.
- To convert PSTN called direct inward dialings (DIDs) to internal directory numbers on incoming PSTN calls, use called party transformation masks in a translation pattern, or limit the significant digits on the appropriate gateway.
- In a multisite deployment with centralized Cisco Unified Communications Manager, it is sometimes necessary to have overlapping endpoint directory numbers in several locations. To handle these overlapping endpoint directory number issues, you can use called party transformation masks in a translation pattern, together with partitions and calling search space (CSS) in order to route the calls to the correct destination.

Note Partitions and calling search spaces are described in another lesson of this module.

Cisco Unified Communications Manager Digit Manipulation Flow

This topic describes a few examples of digit manipulation flow.

**Digit Manipulation Flow Example
(Outgoing Call to PSTN)**

Dials: 9-1-303-555-6007

1005
408-555-3005

PSTN

303-555-6007

408-555-3005 is calling

Step	Description
1	Extension 1005 dials 9-1-303-555-6007
2	Dialed number matches 9! Route pattern configured with the following: <ul style="list-style-type: none">- Called party transformations > Discard digits: PreDot- Calling party transformations: 40855530XX- Route to GW
3	Unified CM strips off (discards) digit “9” from the dialed number and sends 13035556007 to PSTN via the GW after modifying the calling party number from 1005 to 4085553005
4	PSTN phone 3035556007 rings and sees 4085553005 as the calling number

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—4-7

The figure shows an example of an internal caller dialing a PSTN number using a PSTN access code “9” followed by the PSTN number, where the following digit manipulations occur:

- Cisco Unified Communications Manager discards the digit “9” before sending the call out to PSTN.
 - The internal extension calling party number will be expanded to the full PSTN number.
- Simple called and calling party transformations are used in the PSTN route pattern to achieve these two objectives.

Digit Manipulation Flow Example (Incoming Call from PSTN)

The figure shows an example of digit manipulation flow for incoming calls from the PSTN.

Digit Manipulation Flow Example (Incoming Call from PSTN)

Step	Description
1	PSTN phone dials 1-408-555-3010, PSTN switch routes the call to GW/Unified CM
2	Incoming call dialed number matches 40855530XX translation pattern configured with the following: <ul style="list-style-type: none">- Called Party transformation > Called Party Transform Mask: 10XX- (Optional) Calling Party transformation > Prefix Digit: 91
3	<ul style="list-style-type: none">- Unified CM translates 4085553010 to 1010- Unified CM looks up 1010 and finds a registered phone with that directory number
4	Unified CM presents the call to extension 1010. It will (optionally, see Step 2) prefix the calling number with 91 to make it easier for the internal user to call back the PSTN caller from IP phone Directory button (no need to manually add 91)

In the example, an incoming PSTN call to an internal phone is routed as follows:

- The PSTN phone calls the full E.164 number of the destination; the call is received by the PSTN gateway with 10 digits and passed on to Cisco Unified Communications Manager.
- The full PSTN number is converted to the internal number using the called party transformation mask of a translation pattern which covers the full DID range. The resulting number will match an internal extension and Cisco Unified Communications Manager will forward the call to the IP phone registered with the appropriate extension.
- The IP phone will receive the call and the call will be listed in the Received Calls menu. To make it easier for the IP phone user to call back the number, you can use a calling party transformation mask in the same translation pattern to insert “91” to the caller number. This step is optional because the IP phone user can always edit the number and manually add access code “9” and long distance code “1” before calling back the PSTN number.

Cisco Unified Communications Manager Digit Manipulation Configuration Elements

This topic describes the elements of digit manipulation configuration.

Digit Manipulation Configuration Elements

Digit Manipulation Element	Characteristics
External Phone Number Mask	Designates the fully qualified E.164 address for the user extension – Part of Calling/Called Transformation settings.
Digit Prefix and Stripping	Prefix or strip dialed digits from a route or translation pattern for outbound calls – Part of Calling/Called Transformation settings.
Transformation Masks	Manipulate the dialed digits or calling party number – Part of Calling/Called Transformation settings.
Translation Pattern	When dialed digits match the translation pattern, Unified CM performs the translation first and then routes the call again. Make use of the Calling/Called Transformation settings for digit manipulation.
Significant Digits	Strip off digits received by Unified CM for incoming calls from a PSTN gateway or from a trunk.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-10

The table in the figure shows the main elements of digit manipulation configuration and their characteristics. These will be explained in detail in the subsequent topics.

Cisco Unified Communications Manager External Phone Number Mask

This topic describes the Cisco Unified Communications Manager external phone number mask.

External Phone Number Masks

- Designates the fully qualified E.164 address for the user extension
- Used to format caller ID information for external (outbound) calls that are made from the internal devices
- Configured under [Line Configuration](#) settings, but enabled as part of [Calling Party Transformations](#) settings.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-12

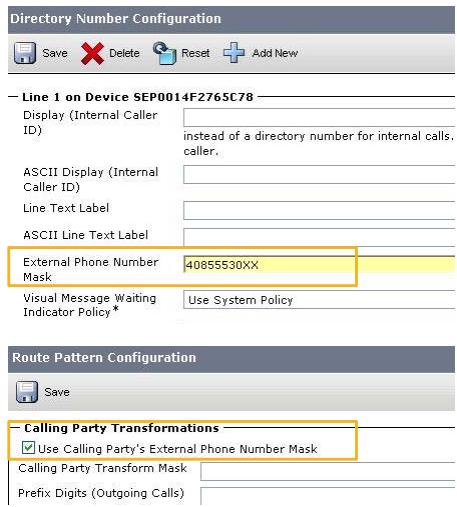
The external phone number mask instructs the call-routing component to use the external (PSTN) phone number of a calling IP phone rather than its internal directory number for the caller ID information. The external phone number mask is set on a line-by-line basis at the directory number configuration screen of a device, and the use of the external phone number mask is enabled globally per PSTN route pattern.

Configuring External Phone Number Mask

The figure illustrates how to configure the external phone number mask on a line and enable its use at route patterns.

Configuring External Phone Number Mask

- Go to **Device > Phone > Find** and select the corresponding phone
- Under **Association Information**, click the corresponding **Line**
- Scroll down to **Line x on Device** configuration (see picture)
- Type full E.164 PSTN number in the **External Phone Number Mask** field
- In the Route Patterns that point to PSTN (e.g. **9.! or 9.@**), scroll to **Calling Party Transformations**
- Check the **Use Calling Party's External Phone Number Mask** option

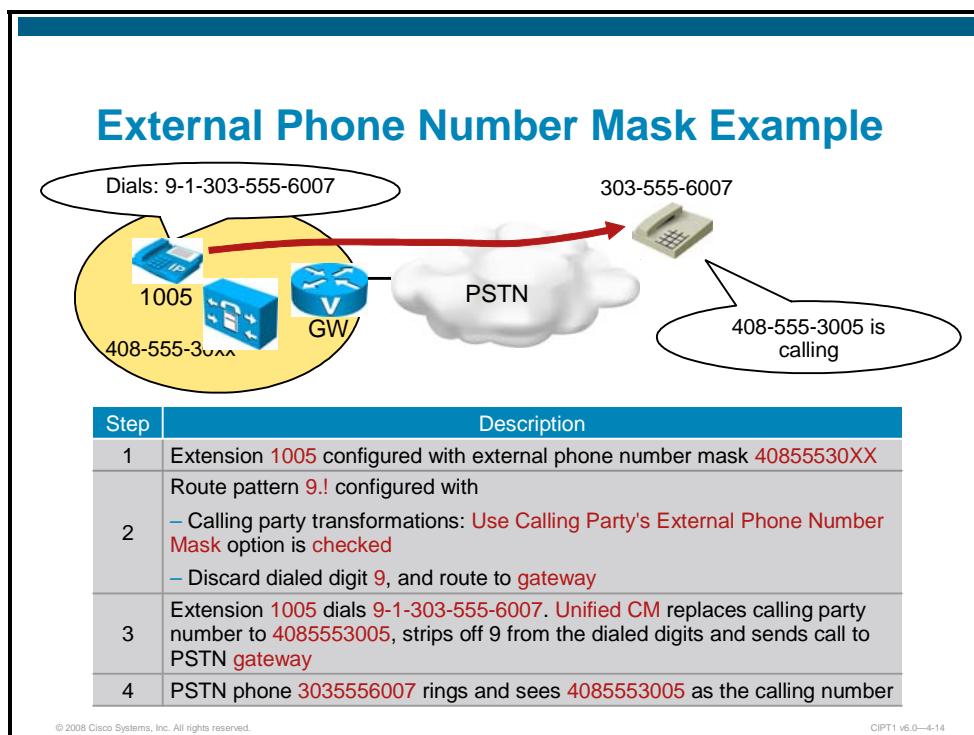


The figure consists of two screenshots. The top screenshot is titled 'Directory Number Configuration' and shows a form for 'Line 1 on Device SEP0014F2765C78'. It includes fields for 'Display (Internal Caller ID)', 'ASCII Display (Internal Caller ID)', 'Line Text Label', 'ASCII Line Text Label', and 'External Phone Number Mask' (which contains the value '40855530XX'). The bottom screenshot is titled 'Route Pattern Configuration' and shows a section for 'Calling Party Transformations'. It includes a checkbox labeled 'Use Calling Party's External Phone Number Mask' which is checked, and other fields for 'Calling Party Transform Mask' and 'Prefix Digits (Outgoing Calls)'.

The above screenshots show how to use the external phone number mask. First, go to each device and configure the full E.164 PSTN number under External Phone Number Mask setting for each line. Then, on each route pattern that points to the PSTN, go to the calling party transformation and check the **Use Calling Party's External Phone Number Mask** check box.

External Phone Number Mask Example

This subtopic shows an example of using the external phone number mask on outgoing PSTN calls.



The figure shows a step-by-step example and description on the use of an external phone number mask.

Cisco Unified Communications Manager Digit Prefix and Stripping

This topic describes how to prefix and strip digits to and from called and calling party numbers in Cisco Unified Communications Manager.

The screenshot shows the Cisco Unified Communications Manager configuration interface. The main title is "Digit Prefix". Below it, a bulleted list defines the feature: "Prepend digits to the pattern", "Valid entries include the digits 0 through 9, *, and #", and "Part of **Calling/Called Transformations** settings". Under "Calling Party Transformations", there is a checkbox for "Use Calling Party's External Phone Number Mask" and several dropdown menus for "Calling Party Transform Mask", "Prefix Digits (Outgoing Calls)" (which is highlighted with a yellow box), "Calling Line ID Presentation*", "Calling Name Presentation*", "Calling Party IE Number Type*", and "Calling Party Numbering Plan*". Under "Called Party Transformations", there is a dropdown menu for "Discard Digits" (set to "< None >"), a dropdown menu for "Called Party Transform Mask", a dropdown menu for "Prefix Digits (Outgoing Calls)" (highlighted with a yellow box), and dropdown menus for "Called Party IE Number Type*" and "Called Party Numbering Plan*" (both set to "Cisco CallManager").

The digit prefix feature prepends digits to a number. Any phone keypad digits from 0–9, as well as * and # digits, can be prepended to the calling and called numbers.

The digit prefix feature can be applied to a calling party or a called party number and configured under the corresponding transformation setting in the route pattern or translation pattern configuration.

Digit Stripping

The digit stripping feature is used to strip digits from a dialed (called party) pattern.

Digit Stripping

- Used to strip digits from a pattern
- Part of **Called Party Transformations** settings (**Discard Digits** field)
- A discard digits instruction (DDI) removes a portion of the dialed digit string before passing the number on
- If no @ sign (numbering plan) is used in route pattern, only the following DDIs are supported:
 - PreDot
 - NoDigits

Called Party Transformations

Discard Digits	< None >
Called Party Transform Mask	
Prefix Digits (Outgoing Calls)	
Called Party IE Number Type*	Cisco CallManager
Called Party Numbering Plan*	Cisco CallManager

DDI

```
PreDot
10-10-Dialing
PreDot 10-10-Dialing
PreAt
PreAt 10-10-Dialing
11D->10D
PreDot 11D->10D
PreDot 11/10D->7D
PreAt 11D->10D
PreAt 11/10D->7D
PreAt 11/10D->7D
IntTollBypass
PreDot IntTollBypass
PreAt IntTollBypass
PreDot Trailing-#
PreDot IntTollBypass Trailing-#
PreAt 11/10D->7D Trailing-#
PreAt Trailing-#
PreAt IntTollBypass Trailing-#
PreAt 10-10-Dialing Trailing-#
```

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-17

A DDI removes part of the dialed digit string, for example, when an access code is needed to route the call to the PSTN but the PSTN switch does not expect that access code. The DDI then passes the number on to the adjacent system.

Digit stripping is configured under the called party transformations by selecting a DDI. It can be configured at route patterns and at route groups of a route list.

For North American Numbering Plan (NANP) patterns (@), the entire range of DDIs is supported. With non-@ patterns, only the <None>, NoDigits, and PreDot DDIs can be used.

Note	<None> means that no DDI is configured at the route pattern, but is permitted in the route group configuration of a route list. NoDigits means that any DDI configured at a route group of a route list has to be ignored. In all other cases, the DDI at the route group of a route list has higher priority than the DDI configured at the route pattern.
-------------	---

In order for the PreDot DDI to work, the route pattern has to include a “.” sign, which is not dialed but used by Cisco Unified Communications Manager to determine how many digits to strip (all digits before the dot).

Understanding DDIs

This subtopic describes some DDIs that are available in Cisco Unified Communications Manager.

Discard Digits Instructions (DDIs)

For example, If the pattern is **9.5@**

Instructions	Discarded Digits	Used for
PreDot	<u>9</u> 5 1 214 555 1212	Removes access code digit(s) delimited by . sign
PreAt	<u>95</u> 1 214 555 1212	Removes all digits that are in front of a valid numbering plan pattern
11D/10D@7D	<u>95 1 214</u> 555 1212	Removes PreDot/PreAt digits and local or long-distance area code
11D@10D	<u>95 1</u> 214 555 1212	Removes long distance area code identifier (1)
IntlTollBypass	<u>95 011 33</u> 1234 #	Removes international access (011) and following country code
10-10-Dialing	<u>95 1010321</u> 1 214 555 1212	Removes carrier access (1010) and following carrier ID code
Trailing-#	95 1010321 011 33 1234 <u>#</u>	Removes of dialed # sign (to terminate dialing without timeout)

© 2008 Cisco Systems, Inc. All rights reserved.

CPT1 v6.0—4-18

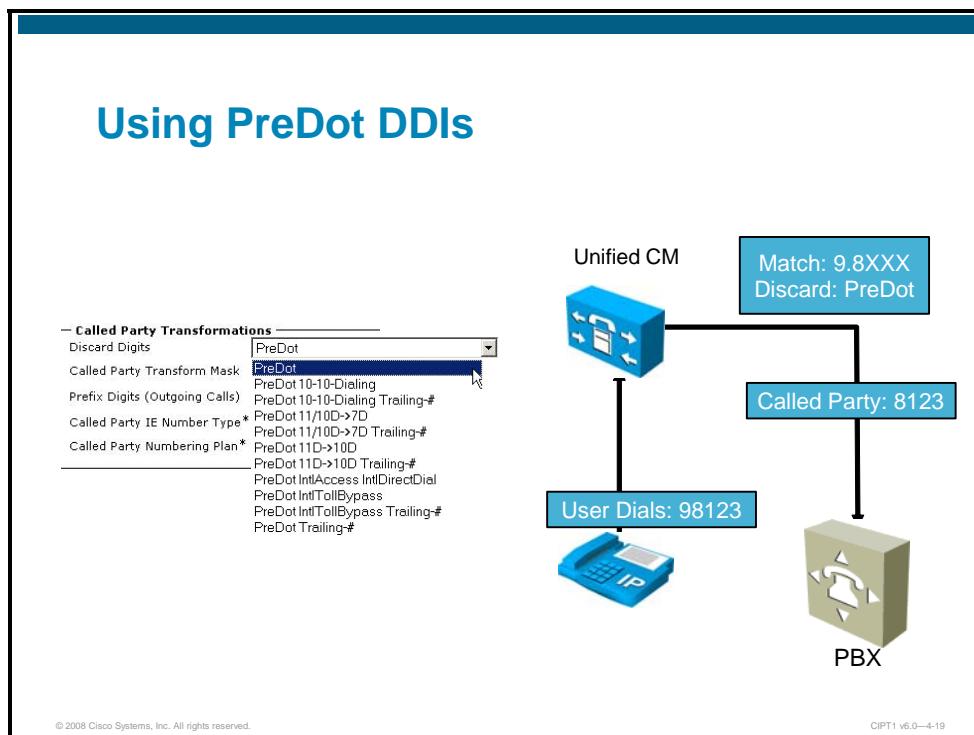
The table in the figure lists the most important examples of DDIs supported in Cisco Unified Communications Manager and explains how they work.

Note

Trailing # is automatically removed by default by Cisco Unified Communications Manager. This behavior can be controlled via the **Service Parameter > Call Manager > Clusterwide Parameters (Device – General) > Strip # Sign from Called Party Number** service parameter which can be set to True (default) or False.

Using PreDot DDIs

This subtopic describes the PreDot DDI.



PreDot and NoDigits DDIs are the only DDIs that can be used if the pattern *does not* contain the @ sign.

In the example in the figure, Cisco Unified Communications Manager applies the PreDot DDI to the 9.8xx route pattern, strips the 9 from the dialed digits, and sends only the 8123 to the PBX.

In Cisco Unified Communications Manager Administration, the Discard Digits menu shown in the figure is available by going to **Call Routing > Translation Pattern** or **Call Routing > Route Pattern**.

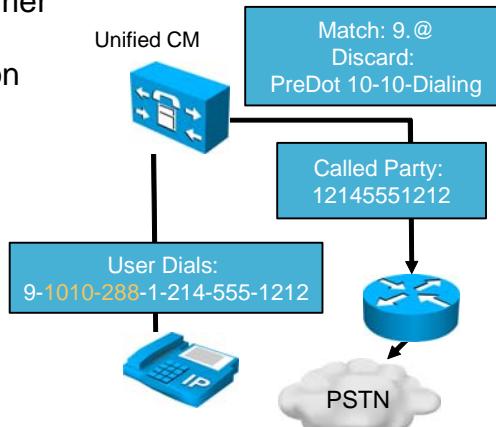
Using Compound DDIs

This subtopic discusses compound DDIs.

Using Compound DDIs

Use DDIs to remove carrier selection from dialed number. Carrier selection consists of:

- Carrier Access Code: 1010
- Carrier Identification Code: 3 digits



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-20

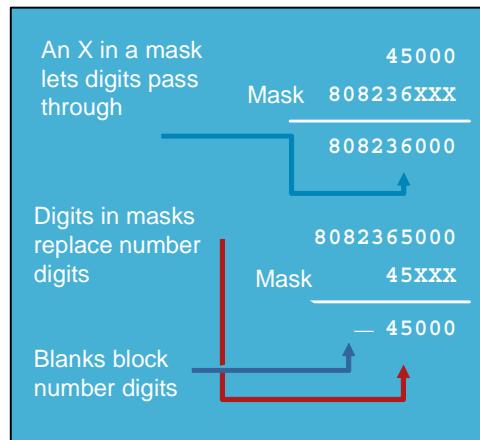
In this example, Cisco Unified Communications Manager applies the PreDot 10-10-Dialing DDI to the 9.@" route pattern. This compound DDI performs two functions: First, it strips the access code 9 from the dialed number (9-1010-288-1-214-555-1212), then it removes the carrier selection (dialed by Carrier Access Code 1010 followed by a 3-digit Carrier Identification Code, in this case 288) and sends only 1-214-555-1212 to the gateway device.

Cisco Unified Communications Manager Transformation Masks

This topic describes transformation masks in Cisco Unified Communications Manager.

Transformation Masks

- Modify either the calling number or called number (dialed digits)
- Can contain digits 0–9, *, #, and X
- Applied to a number to extend or truncate it
- Part of **Calling/Called Party Transformations** settings



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-22

Dialing transformations allow the call-routing component to modify either the calling number or the dialed digits of a call. Transformations that modify the calling number are “calling-party transformations”; transformations that modify the dialed digits are “called-party transformations.”

Transformation masks use mask operations to allow the suppression of leading digits, the change of some digits while leaving others unmodified, and the insertion of leading digits.

A mask operation requires two items of information: the number to mask and the mask itself.

In the mask operation, Cisco Unified Communications Manager overlays and aligns the number with the mask so that the last character of the mask aligns with the last digit of the number. Cisco Unified Communications Manager uses the corresponding digit of the number wherever the mask contains an X. If the number is longer than the mask, the mask obscures the extra digits.

Note	Cisco Unified Communications Manager also allows the configuration of called translation patterns, which translate dialed numbers by also using transformation masks. The main differences in these two mask operations (route pattern with called party transformation and translation pattern with called party transformation) are that, first, a called party transformation is mandatory in translation patterns because the modification of the called number is the function of a translation pattern, and next, the called party transformation of a route pattern is only used to modify the called party number in the signaling messages that are sent to the destination device configured at the route pattern (gateway, trunk, and so on) but no additional routing request is generated. A translation pattern, on the other hand, modifies the dialed number and generates a new routing request for the translated number.
-------------	---

Configuring Transformation Masks

This subtopic describes how to configure transformation masks.

Configuring Transformation Masks

- Configured under **Translation Pattern, Route Pattern, or Route List** settings
- Transformation masks configured at route list level have priority over those configured at route pattern level

— Calling Party Transformations —

Use Calling Party's External Phone Number Mask
Calling Party Transform Mask

Prefix Digits (Outgoing Calls) _____
Calling Line ID Presentation* Default
Calling Name Presentation* Default
Calling Party IE Number Type* Cisco CallManager
Calling Party Numbering Plan* Cisco CallManager

— Connected Party Transformations —

Connected Line ID Presentation* Default
Connected Name Presentation* Default

— Called Party Transformations —

Discard Digits < None >
Called Party Transform Mask

Prefix Digits (Outgoing Calls) _____
Called Party IE Number Type* Cisco CallManager
Called Party Numbering Plan* Cisco CallManager

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-23

Transformation masks are configurable at route patterns, translation patterns, and per route group at route lists.

The calling-party and called-party transformation settings that are assigned to route groups in a route list override the corresponding transformation settings that are assigned to a route pattern associated with that route list.

Transformation masks are usually applied at the route list level. In this way, a different transformation mask can be assigned for each route group in the route list.

For example, a network administrator has created two route groups: the PSTN route group and the IP WAN route group. Both of these route groups contain multiple gateways that connect to their respective networks. When Cisco Unified Communications Manager forwards a call to a gateway in the PSTN route group, the network administrator applies a mask that transforms the number into an E.164-compliant phone number. However, when Cisco Unified Communications Manager uses a gateway from the IP WAN route group, Cisco Unified Communications Manager leaves the number as a four-digit extension.

Cisco Unified Communications Manager Translation Patterns

This topic describes the functionality and configuration of translation patterns.

Translation Patterns

- Very powerful tool to manipulate dialed digits and calling party number for any type of call.
- Can be used to either **route** or **block** certain patterns.
- When the digits match the translation pattern, Cisco Unified Communications Manager does not route the call to an outside entity (e.g., a gateway); instead, it performs the translation first and then routes the call (to another translation pattern or to a route pattern).

© 2008 Cisco Systems, Inc. All rights reserved.

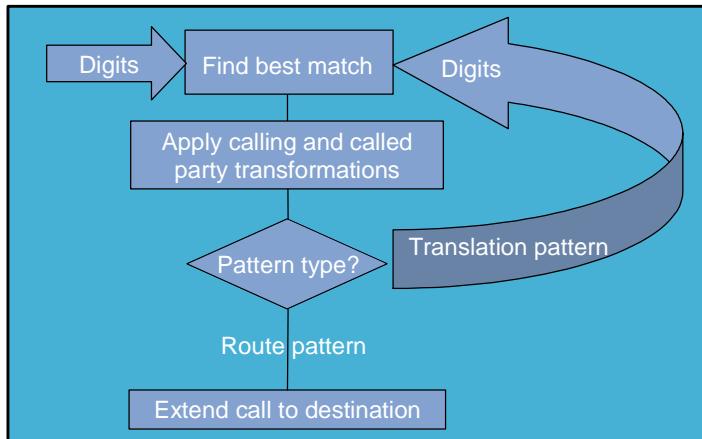
CIPT1 v6.0—4-25

Cisco Unified Communications Manager uses translation patterns to manipulate dialed digits before routing a call or to manipulate the calling party number. In some cases, the dialed number is not the number that is used by the system. In other cases, the dialed number is not a number that is recognized by the PSTN. The translation pattern also can be used to block certain patterns.

Digit manipulation and translation patterns are used frequently in cross-geographical distributed systems where, for instance, the office codes are not the same at all locations. In these situations, a uniform dialing plan can be created and translation patterns applied to accommodate the unique office codes at each location. Additional examples where translation patterns can be used are as follows:

- Security desks and operator desks
- Hot lines with a need for private line, automatic ringdown (PLAR) functionality
- Extension mapping from the public to a private network

Translation Patterns (Cont.)



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-26

Translation patterns use the results of called-party transformations as a set of digits for a new analysis attempt. The second analysis attempt might match a translation pattern. In this case, Cisco Unified Communications Manager applies the calling- and called-party transformations of the matching translation pattern and uses the results as the input for another analysis attempt. To prevent routing loops, Cisco Unified Communications Manager breaks chains of translation patterns after 10 iterations.

Configuring a Translation Pattern

This subtopic describes the configuration of a translation pattern.

Configuring Translation Pattern

- Go to **Call Routing > Translation Pattern > Add New**
- Enter the **Translation Pattern**, including numbers and wildcards (do not use spaces)
- Choose a **Partition** and **CSS** (to be discussed in the next module) or choose **<None>**
- Choose the **Route Option** to indicate this pattern is to be used for routing or for blocking calls (the “blocking” option provides similar functionality as in the Route Pattern configuration)
- Specify the **Calling/Called Party Transformation** settings (applicable only if “Route the pattern” is selected above)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-27

Configuration of a translation pattern is similar to configuration of a route pattern. Each pattern has calling- and called-party transformations settings. The difference is that when Cisco Unified Communications Manager applies the translation pattern, it starts the digit analysis process over to perform another call routing process for the modified number.

To configure a translation pattern, choose the **Call Routing** menu and choose **Translation Pattern**. The route pattern can be defined to match and the calling- or called-party transformation settings that should be applied.

If you click the Block this Pattern radio button, you must select the reason for translation pattern to block calls. Choose one of these values from the drop-down list:

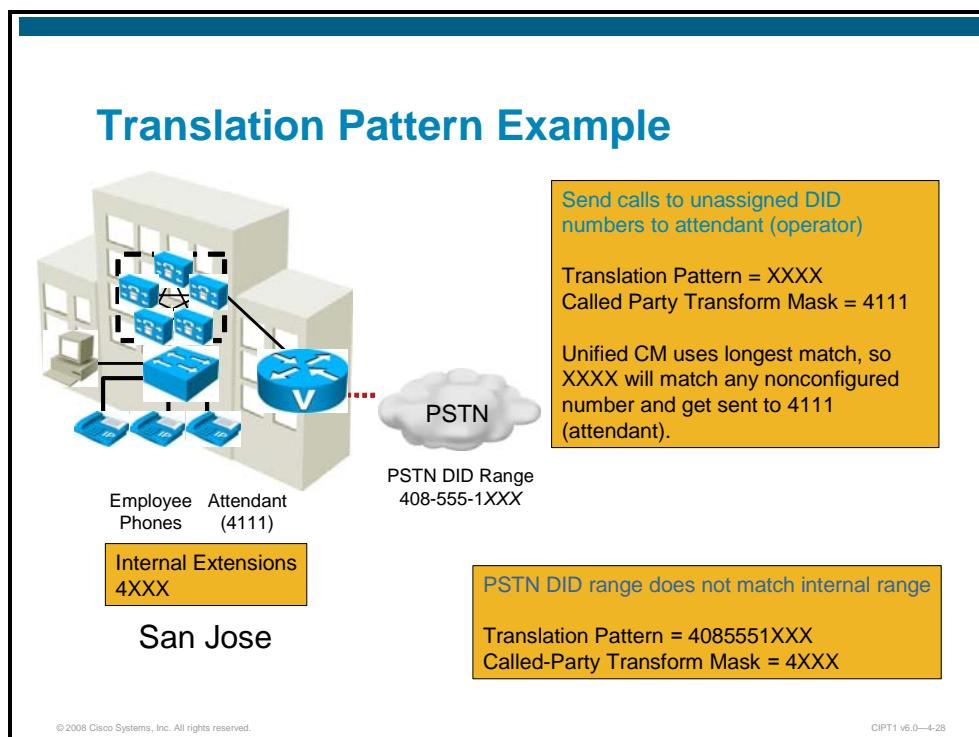
- No Error
- Unallocated Number
- Call Rejected
- Number Changed
- Invalid Number Format
- Precedence Level Exceeded

The transformation settings are not applicable if the Block this Pattern radio button is selected.

If the translation pattern contains an @ sign, you can select a Numbering Plan and Route Filter to match certain number patterns of the selected numbering plan.

Translation Pattern Example

The figure shows an application for translation patterns.



When the DID range from the central office (CO) does not match the internal directory number range, a translation pattern can be used to map dialed DIDs to internal directory numbers.

In the figure, a San Jose, California, company has a PSTN DID range of 408-555-1XXX. However, all of the internal four-digit extensions begin with 4XXX. When the company receives an incoming call, the company can use a translation pattern that matches the assigned PSTN DID range (408-555-1XXX) and has a transformation mask 4XXX. This mask converts the dialed 408-555-1XXX PSTN numbers to a 4XXX internal range, conserving the last three digits. After Cisco Unified Communications Manager applies the transformation mask, it performs a new call routing lookup for the translated four-digit number, finds the directory number in its call routing table, and routes the call to the corresponding IP phone.

In addition, there is a translation pattern XXXX with a called-party transformation mask of 4111. This pattern routes calls placed to unassigned directory numbers to 4111 (that is, the directory number of the attendant). Assume that directory number 4333 does not exist and an internal user dials 4333. Because no directory number with 4333 exists, the translation pattern XXXX is the best match and the call is rerouted to 4111. The same happens for outside callers dialing to 408-555-1333. Such a call first matches the translation pattern 408-555-1XXX and therefore gets translated to 4333. After the translation, the call is handled like the internal call placed to 4333—it does not find a directory number entry and therefore matches XXXX again. The call is again rerouted to 4111.

Cisco Unified Communications Manager Significant Digits

This topic describes the use of the Significant Digits feature of Cisco Unified Communications Manager.

Significant Digits

- Instruct Cisco Unified Communications Manager to pay attention to only the least-significant N digits of the called number for incoming calls from PSTN or from another Cisco Unified Communications Manager cluster
- Part of **gateway** and **trunk** configuration
- Affects **all** incoming calls received by the gateway or trunk; not recommended for variable-length extension numbers

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-30

The Significant Digits feature instructs Cisco Unified Communications Manager to pay attention to only the least-significant N digits of the called number for incoming calls received by a gateway or a trunk. For example, setting the Significant Digits to 5 on a PSTN gateway will cause Cisco Unified Communications Manager to ignore all but the last five digits of the called number for incoming PSTN calls. This is the easiest approach to converting incoming PSTN called-numbers to the internal extension, but it affects all calls received from that gateway. Thus, if there are variable-length extension numbers, this is not the recommended approach.

Configuring Significant Digits

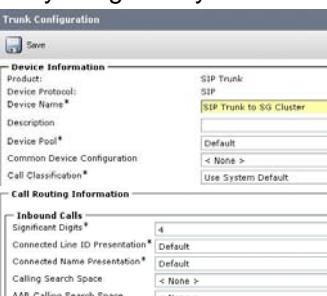
This subtopic describes how to configure the Significant Digits feature.

Configuring Significant Digits

- Go to **Gateway or Trunk Configuration > Call Routing Information – Inbound Calls**
- In the **Significant Digits** field, specify the last **N** digits of the called number that you want Cisco Unified Communications Manager to process for inbound calls received by the gateway or trunk



The screenshot shows the 'Gateway Configuration' window. Under 'Device Information', it lists fields like 'Gateway' (gw1.domain.com), 'Device Protocol' (Digital Access PRI), and 'IP Address' (Unknown). Under 'Call Routing Information - Inbound Calls', there is a 'Significant Digits' field set to '4'. Other fields include 'Calling Search Space', 'AAR Calling Search Space', 'Prefix DN', and 'Calling Party Transformation CSS' (with a checked checkbox for 'Use Device Pool Calling Party Transformation CSS').



The screenshot shows the 'Trunk Configuration' window. Under 'Device Information', it lists fields like 'Product' (SIP Trunk), 'Device Protocol' (SIP), and 'Device Name' (SIP Trunk to SG Cluster). Under 'Call Routing Information - Inbound Calls', there is a 'Significant Digits' field set to '4'. Other fields include 'Connected Line ID Presentation', 'Connected Name Presentation', 'Calling Search Space', 'AAR Calling Search Space', and 'Prefix DN'.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—4-31

The Significant Digits feature is configured under the Gateway Configuration or Trunk Configuration windows and affects all incoming calls received by the gateway or trunk.

Go to **Gateway Configuration or Trunk Configuration > Call Routing Information – Inbound Calls**, and, in the Significant Digits field, specify the last N digits of the called number that Cisco Unified Communications Manager should process for incoming calls received by the PSTN gateway or trunk.

Significant Digits Example

This topic shows an example of the Significant Digits feature.

Significant Digits Example

The diagram shows a PSTN gateway (GW) receiving a call from a PSTN phone (303-555-6008). The PSTN gateway routes the call to a Cisco Unified Communications Manager (CUCM) gateway. The CUCM gateway is configured with significant digits = 4. It strips off the first three digits (408) and routes the call to an IP phone (1010) based on the last four digits (555-1010).

Step	Description
1	PSTN phone dials 1-408-555-1010. PSTN switch routes the call to gateway.
2	PSTN gateway device configured with the following: <ul style="list-style-type: none">Significant Digits = 4
3	Cisco Unified Communications Manager will ignore all but the last 4 digits of the called number (1010).
4	Cisco Unified Communications Manager looks up 1010 and finds a registered phone with that directory number and presents the call to extension 1010.

In the example in the figure, the PSTN gateway receives an incoming call with the destination number of 408-555-1010 through a gateway. If Significant Digits = 4 is configured in the gateway configuration in Cisco Unified Communications Manager, Cisco Unified Communications Manager will strip off all digits except the last four digits (1010), look up this number (1010) in its call routing table, and forward the call to the IP phone configured with that directory number.

Note	In contrast to using translation patterns to map dialed E.164 numbers to internal directory numbers on incoming PSTN calls, this solution performs only one call routing table lookup. On the other hand, significant digits can only be used if all the significant digits are the same (that is, the full directory number is also used in the DID range). If the PSTN DID range (for example, 1XXX) is different than the directory numbers used for the phones (4XXX), translation patterns are required and significant digits cannot be used.
-------------	---

Cisco Unified Communications Manager Digit Manipulation

This topic describes the use of transformation settings and the order in which Cisco Unified Communications Manager processes those instructions.

Transformation Settings

- **Calling Party Transformations** control the adaptation of calling party numbers from enterprise format to PSTN format
- **Called Party Transformations** manipulate the dialed digits, Number Type, and Numbering Plan.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-34

The transformation configuration can be broken down into two separate tasks:

- Calling Party Transformation controls the adaptation of calling party numbers.
- Called Party Transformation manipulates the dialed digits.

Calling Party Transformation Order

The example in the figure shows the applicable settings for calling-party transformations and the order in which Cisco Unified Communications Manager processes those instructions.

The screenshot shows the 'Calling Party Transformation Order' configuration interface. On the left, a list of steps is provided:

1. Apply the external phone number mask
2. Apply the calling party transformation mask
3. Apply prefix digits

On the right, the configuration details are displayed in a table:

Directory Number	35062
External Phone Number Mask	21471xxxxx
Calling-Party Transformation Mask	2147135062
Caller ID	40885xx000
	4088535000

Below the table, under 'Calling Party Transformations', the following settings are shown:

- Use Calling Party's External Phone Number Mask
- Calling Party Transform Mask: 40885XX000
- Prefix Digits (Outgoing Calls): (empty)
- Calling Line ID Presentation*: Default
- Calling Name Presentation*: Default
- Calling Party IE Number Type*: Cisco CallManager
- Calling Party Numbering Plan*: Cisco CallManager

At the bottom of the interface, the copyright notice is '© 2008 Cisco Systems, Inc. All rights reserved.' and the page number is 'CIPT1 v6.0—4-35'.

Three types of calling-party transformations can be configured at route patterns and per route group in a route list, in the following order:

1. The external phone number mask instructs the call-routing component to use the external phone number of a calling station rather than its directory number or the caller ID information. The external phone number mask can be applied on a line-by-line basis through the directory number configuration screen on the device.
2. The calling-party transformation mask suppresses leading digits, leaving other digits unmodified, or inserts leading digits.
3. Prefix digits allow prepending of specified digits to the calling number.

Cisco Unified Communications Manager applies the transformations in the order that is presented in the example.

Note	This is not a realistic example. It is useless and confusing to assign an external phone number mask that is then changed to a completely different number (different area code). The numbers in the example are only used for a better illustration of the transformation process. They should not be considered to be useful in a realistic scenario.
-------------	---

Called Party Transformation Order

The example in the figure shows the applicable settings for called-party transformations and the order in which Cisco Unified Communications Manager processes those instructions.

The screenshot displays the 'Route Pattern Configuration' screen under 'Called Party Transformations'. On the right, a large blue box illustrates the transformation process:

Dialed Number	9 1010321 18085551221
Discard Digits	10-10-Dialing
	9 18085551221
Called-Party Transformation Mask	XXXXXXXXXXXX
	8085551221
Prefix Digits	8
Called Number	88085551221

The left side of the interface shows the configuration details for the route pattern:

- Pattern Definition:**
 - Route Pattern: 9,@
 - Route Partition: < None >
 - Description: (empty)
 - Numbering Plan: -- Not Selected --
 - Route Filter: < None >
 - MLPP Precedence: Default
- Called Party Transformations:**
 - Discard Digits: 10-10-Dialing
 - Called Party Transform Mask: XXXXXXXXXX
 - Prefix Digits (Outgoing Calls): 8
 - Called Party IE Number Type: Cisco CallManager
 - Called Party Numbering Plan: Cisco CallManager

At the bottom of the interface, there are copyright and version information: © 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—4-36

Three types of called-party transformations can be configured in the call-routing component and on route lists:

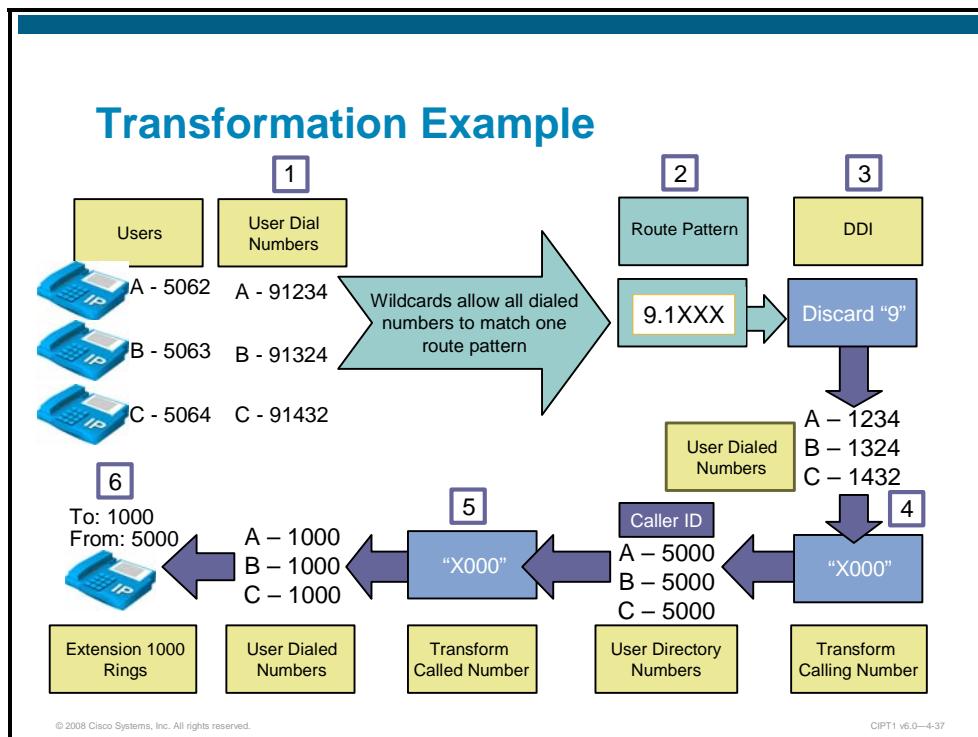
- DDIs allow the discarding of subsections of a numbering plan, such as the NANP. They can also be used to discard PSTN access codes, such as 9.
- The called-party transformation mask allows the suppression of leading digits, changes the existing digits while leaving others unmodified, or inserts leading digits.
- Prefix digits allow prepending of one or more digits to the called number.

If multiple transformations are configured, Cisco Unified Communications Manager applies the transformations in the following order as presented in the example:

1. DDI first discards the digits from the dialed number.
2. Transformation then continues; the called-party transformation mask adds or removes additional digits.
3. Finally, the prefix is added at the beginning of the number.

Transformation Example

The figure shows how transformations to the called-party (dialed digits) and to the calling-party numbers are made in Cisco Unified Communications Manager.



In the figure, a user dials a number to which Cisco Unified Communications Manager first applies a calling-party transformation. This action changes the caller ID number that is displayed on the destination phone. Cisco Unified Communications Manager then applies a called-party transformation to change the number that is dialed.

The two transformations are explained in the figure and, for user A specifically, in these steps:

- Step 1** User A has a directory number 5062. This user dials 91234.
- Step 2** The dialed number matches the route pattern 9.1xxx.
- Step 3** The DDIs contain instructions to discard the 9. The dialed number is now 1234.
- Step 4** The calling number 5062 now passes through the calling-number transformation mask, which contains instructions to change the last three digits of the calling party number to 000. The new calling number is 5000.
- Step 5** Cisco Unified Communications Manager then passes the called number 1234 through the called-number transformation mask X000, which changes this number to 1000.

The result is a calling-party number 5000 and a called-party number 1000.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- In many call scenarios, it is required to manipulate the calling and called (dialed) string before routing the call.
- Cisco Unified Communications Manager digit manipulation configuration main elements are: External Phone Number Mask, Digit Prefix and Stripping, Transformation Masks, Translation Pattern, and Significant Digits.
- Cisco Unified Communications Manager External Phone Number Mask designates the fully qualified E.164 address for the user's extension and is used to format Caller-ID information for outbound calls from the internal devices.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-38

Summary (Cont.)

- Digit Prefix prepends digits to a pattern, Digit Stripping strips digits from a pattern.
- Transformation Masks modify either the calling number or the called number (dialed digits).
- Translation Pattern can be used to either route or block certain patterns. When the digits match the translation pattern, Cisco Unified Communications Manager performs the translation first before routing the call to another translation pattern or to a route pattern.
- Significant Digits instruct Cisco Unified Communications Manager to pay attention to only the least-significant N digits of the called number for incoming calls from PSTN or from another Cisco Unified Communications Manager cluster.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-39

References

For additional information, refer to these resources:

- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf

Lesson 4

Implementing Calling Privileges in Cisco Unified Communications Manager

Overview

Calling privileges are an important dial plan component. Calling privileges are used to implement class of service (CoS), which means that, based on the calling device or line, some destinations are permitted to access call routing table entries while others are not.

Implementation applications include time-of-day routing, vanity numbers, Client Matter Codes (CMC), Forced Authorization Codes (FAC), and private line, automatic ringdown (PLAR).

This lesson describes the configuration tools that can be used to implement calling privileges and discusses different usage scenarios.

Objectives

Upon completing this lesson, you will be able to explain the need and uses for calling privileges and to implement them in Cisco Unified Communications Manager. This ability includes being able to meet these objectives:

- Describe the tools that Cisco Unified Communications Manager supports for call privilege implementation
- Describe how partitions and calling search spaces work and how they are configured
- Describe how time schedules and time periods work and how they are configured
- Describe how CMC and FAC work and how they are configured
- List applications for calling privileges configuration elements
- Describe how to implement CoS
- Describe how to implement 911 emergency calls and vanity numbers
- Describe how to implement time of day-based carrier selection
- Describe how to implement PLAR

Calling Privileges Fundamentals

This topic describes the fundamentals of calling privileges.

Calling Privileges

Calling privileges (also called class of service) define the entries of a call routing table that can be accessed by an endpoint performing a call routing request.

- Used to control telephony charges
 - Block costly service numbers
 - Restrict international calls
- Used for special applications including:
 - Route calls with the same number differently per user (different gateway per site for PSTN calls)
 - Route calls to the same number differently per time of day

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-4

Calling privileges are configured in order to control which entries of the call routing table are accessible from a particular endpoint (such as a phone, gateway, or trunk). The primary application of calling privileges is the implementation of CoS, which is usually used to control telephony charges by blocking costly service numbers and by blocking international calls for some users, and to protect the privacy of some users (for instance, to disallow direct calls to managers except through their assistants).

Calling privileges can also be used to implement special applications such as routing calls that have been placed to the same number in a different manner because of different calling devices. For example, in a selective public switched telephone network (PSTN) breakout a multisite environment with PSTN gateways at each site, PSTN route patterns should always be routed to the local PSTN gateway, so the same route patterns must exist multiple times (once per site, in this example) and only the site-specific route patterns should be accessible by the devices located at this site.

Another application is time-of-day routing, in which calls should take different paths depending on the time when the call is placed.

Call Privileges Requirement Example

The figure shows an example of calling privileges used to implement class of service.

Calling Privilege Class (Class of Service)	Allowed Destinations
Internal	<ul style="list-style-type: none">▪ Internal▪ Emergency
Local	<ul style="list-style-type: none">▪ Internal▪ Emergency▪ Local PSTN
Long Distance	<ul style="list-style-type: none">▪ Internal▪ Emergency▪ Local PSTN▪ Long Distance PSTN
International	<ul style="list-style-type: none">▪ Internal▪ Emergency▪ Local PSTN▪ Long Distance PSTN▪ International PSTN

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-5

The figure shows a typical class of service implementation with calling classes and their allowed destinations. These calling classes can then be assigned to devices or users.

In the example in the figure, class Internal allows only internal and emergency calls. Class Local adds the permission for local PSTN calls, class Long Distance also allows long-distance PSTN calls and class International also enables international PSTN calls.

Calling Privileges Configuration Elements

The table in the figure lists configuration elements that are used for calling privilege implementation along with their characteristics.

Call Privileges Configuration Elements	
Call Privileges Element	Characteristics
Partitions	Group of numbers (directory numbers, route patterns, translation patterns, etc.) with similar reachability characteristics
Calling Search Spaces (CSSs)	Defines which partitions are accessible to a particular device
Time Schedules and Time Periods	Used to allow certain partitions to be reachable only during a certain time of the day
Client Matter Codes (CMC)	Used to track calls to certain numbers A user must enter a Client Matter Code to track calls to certain clients
Forced Authorization Codes (FAC)	Restrict outgoing calls to certain numbers A user must enter an authorization code to reach the number

All of these elements are discussed in more detail in the following topics of this lesson.

Partitions and Calling Search Spaces

This topic describes how partitions and calling search spaces (CSSs) interact with each other and how they are used to implement calling privileges.

Partitions and Calling Search Spaces

- A partition is a group of numbers with same reachability.
 - Any dialable patterns can be part of a partition (directory numbers, route patterns, translation patterns, voice-mail ports, Meet-Me conference numbers, etc.).
- Calling search space is a list of partitions and includes the partitions that are accessible by this CSS.
 - A device can call only those numbers located in the partitions that are part of its calling search space.
 - Assigned to any entity that can generate a call routing request, including phones, phone lines, gateways, and applications.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-8

A partition is a group of dialable patterns with similar accessibility, and a CSS defines which partitions are accessible to a particular device. A device can call only those call routing table entries located in partitions that are part of the CSS of the device.

Partitions are assigned to call routing targets, that is, any entry of the call routing table, including voice-mail ports, directory numbers, route patterns, translation patterns, Meet-Me conference numbers, and so on.

CSSs are assigned to sources of call routing requests such as phone lines, gateways, trunks, voice-mail ports, and applications.

Partition <None> and CSS <None>

This subtopic describes what happens to entities which do not have a partition or CSS assigned.

Partition <None> and CSS <None>

- Before partitions and CSS are configured, all entities that can have a partition (i.e., *called entities* such as directory numbers, route patterns, etc.) reside in partition <None>, and all entities that can have a CSS (*calling entities* such as phones or trunks) are assigned with CSS <None>.
- Entities that are in partition <None> are always accessible (regardless whether the calling entity has a CSS or not).
- Entities that have CSS <None> assigned can only access entities that are in partition <None>.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-9

By default, all entities that can be configured with a partition are in partition <None>, and all entities that can be configured with a CSS are assigned with CSS <None>.

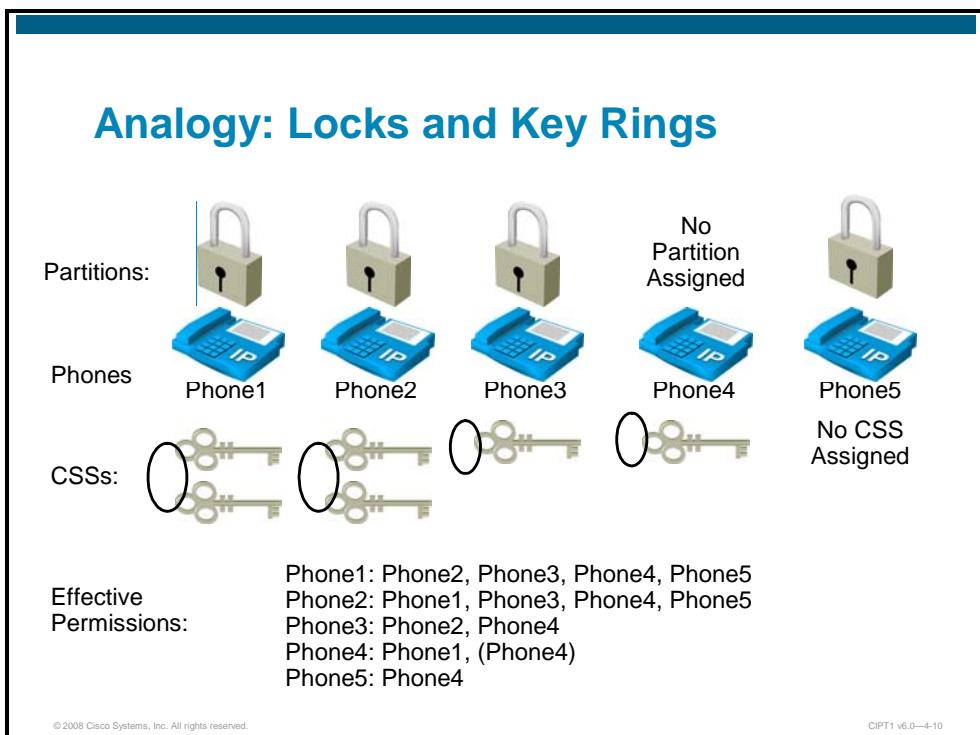
Members of partition <None> (also called the null partition) are always accessible by sources of a call routing request, regardless of the CSS of that call routing source.

Entities that do not have a CSS assigned (that are using CSS <None>) can only access call routing targets that are in partition <None>.

By default, no partitions and CSSs are assigned, and all entities are associated with the null partition and CSS <None>, therefore all calls are possible for all calling sources.

Analogy: Locks and Key Rings

The figure shows the interaction of configured partitions and CSSs, the null partition and CSS <None>.



The example in the figure uses an analogy of locks and key rings. Locks represent partitions applied by the administrator and key rings represent a CSS also configured by the administrator.

In the example, Phone1 has been configured as a member of the blue partition, Phone2 is in the red partition, and Phone3 and Phone5 are in the gold partition. Phone4 has not been assigned to a partition. Following the analogy with locks and keys, you can say that there are three different types of locks (blue, red, and gold), two of them assigned to one phone each and one of them assigned to two phones. Phone4 is not secure with a lock.

When looking at the CSSs as key rings, Phone1 has a key ring with the red and gold key on it, Phone2 has a key ring with the blue and gold key, Phone3 has a key ring with only the red key, Phone4 contains only the blue key, and Phone5 does not have any keys.

As a result of this implementation of locks and keys, the following effective permissions apply:

- **Phone1:** Like all other phones, this phone has access to all devices that do not have a lock applied (Phone4, in this example). In addition, it can unlock red and gold locks because it has the appropriate keys. That means that Phone1 can access Phone2, Phone3, Phone4, and Phone5.
- **Phone2:** Like all other phones, Phone2 has access to all devices that do not have a lock applied (Phone4, in this example). In addition, it can unlock blue and gold locks because it has the appropriate keys. That means that Phone2 can access Phone1, Phone3, Phone4, and Phone5.
- **Phone3:** Like all other phones, this phone has access to all devices that do not have a lock applied (Phone4, in this example). In addition it can unlock red locks because it has the appropriate key. That means that Phone3 can access Phone2 and Phone4.

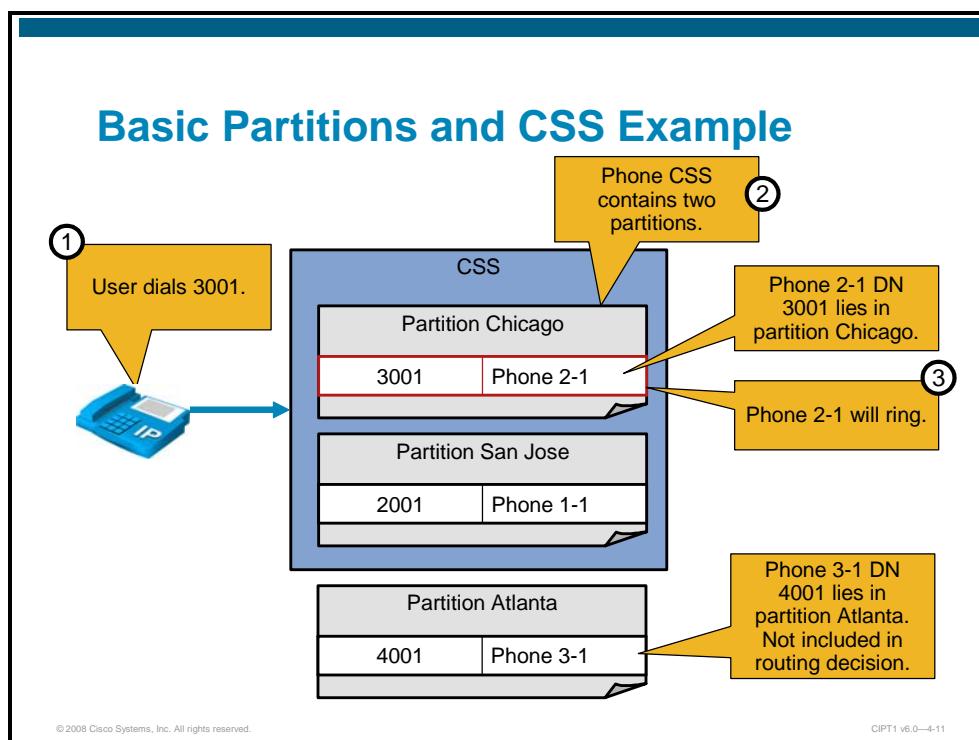
- **Phone4:** Like all other phones, Phone4 has access to all devices that do not have a lock applied (Phone4, in this example). In addition it can unlock blue locks as it has the appropriate key. That means that Phone4 can access Phone1, and itself, which is of no practical importance because Phone4 usually does not place a call to itself.
- **Phone5:** Like all other phones, this phone has access to all devices that do not have a lock applied (Phone4, in this example). Phone5 cannot unlock any locks because it does not have any keys. That means that Phone4 can only access Phone4.

To summarize the analogy used here: Partitions are identical locks, which can be unlocked by the same key, and CSS are key rings that include certain keys. If no lock (partition) is applied to a device, that device can be accessed by everyone. If no keys are present (no CSS configured), only devices that do not have a lock can be accessed.

Note	Calling privilege implementation in Cisco IOS technologies is called class of restriction (COR). The concept is similar to Cisco Unified Communications Manager; however, one difference is that if there is no incoming COR list (which is equivalent to a CSS) all outgoing COR lists (equivalent to partitions) can be unlocked. From the perspective of the presented analogy, it means that if no key ring is applied, all locks can be accessed. COR is discussed in more detail in the CVOICE course.
-------------	--

Basic Partitions and CSS Example

The figure provides an example of partitions and CSSs.



In the example, a phone has a CSS, which contains two partitions, Chicago and San Jose. A third partition, Atlanta, exists but is not included in the CSS of the phone. Phone directory numbers are assigned to partitions as follows:

- Directory number 3001 (Phone 2-1) is assigned to partition Chicago.
- Directory number 2001 (Phone 1-1) is assigned to partition San Jose.
- Directory number 4001 (Phone 3-1) is assigned to partition Atlanta.

The user places a call:

- The user dials 3001, which is the directory number of Phone 2-1.
- Cisco Unified Communications Manager takes the number 3001 and performs a call routing lookup through the partitions configured in the CSS of the calling phone: Chicago and San Jose.
- Cisco Unified Communications Manager finds a match in partition Chicago, because the directory number 3001 of Phone 2-1 is assigned to this partition. Because no other matches exist, routing is complete and Phone 2-1 rings.

Note

Cisco Unified Communications Manager will not even consider the partition Atlanta during the routing decision because it is not included in the CSS.

CSS Partition Order Relevance

This subtopic describes the relevance of the order of partitions within the CSS.

CSS Partition Order Relevance

A CSS is an *ordered* list of partitions.

- All accessible entities of the call routing table are considered by best-match logic.
 - Entities which are in a partition that is listed in the CSS of the calling entity
 - Entities which do not have a partition assigned
- Multiple identical entities can exist in the call routing table but **must be in different partitions**.
- If no single best match, the entry of the call routing table is used whose partition is listed first in the CSS of the calling device.
- Resulting route selection priorities:
 1. Best match
 2. If multiple, equally qualified matches, order of partition is tie breaker

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-12

A CSS is an ordered list of partitions. That is, the partition that is listed first has higher priority than a partition that is listed later. When Cisco Unified Communications Manager performs a call routing lookup, all accessible entities (that is, all targets that reside in a partition listed in the CSS of the calling phone and all targets that do not have a partition applied) are considered by best-match logic.

Multiple identical entities can exist in the call routing table, but they must be in different partitions. One exception to this rule is phone directory numbers. If two or more devices share the same directory number within the same partition, then this is called a shared line.

Note More information about shared lines is provided in a separate module of this course.

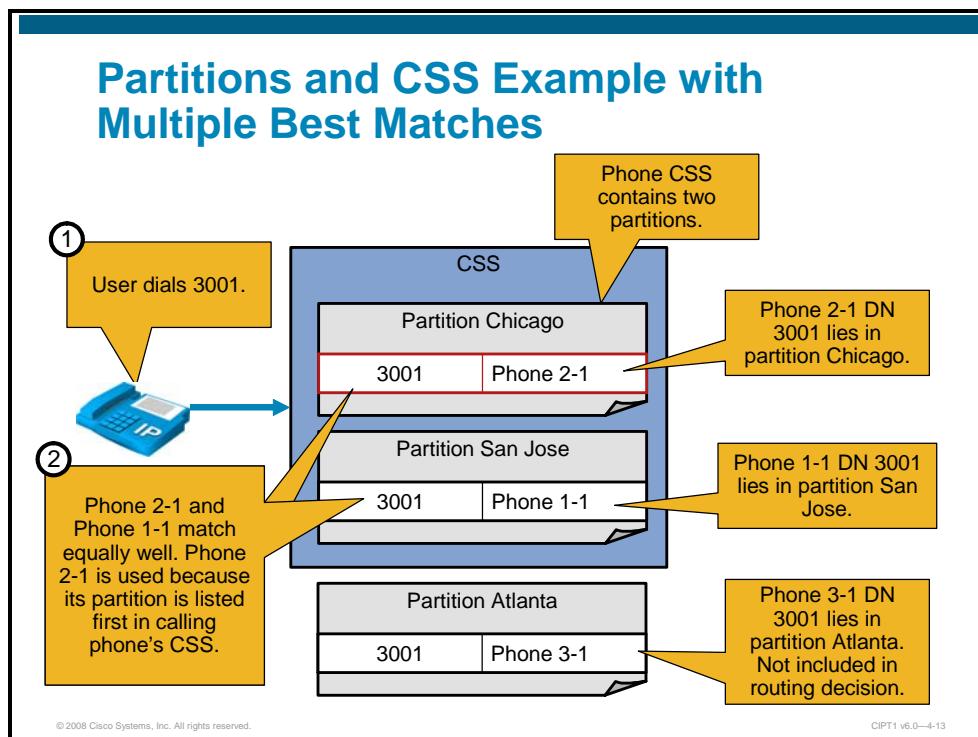
If no single best match is found, the entry of the call routing table is used whose partition is listed first in the CSS of the calling device.

In summary, the entry of the call routing table is selected based on the following order:

- Step 1** Best match.
- Step 2** If multiple equally qualified matches exist (no single best match), the order of the partition in the CSS of the calling device is the tie-breaker (that is, the match that is found in the earlier listed partition).

Partitions and CSS Example with Multiple Best Matches

The figure shows an example in which multiple best matches exist and the call routing decision is based on the order of the partition in the CSS.



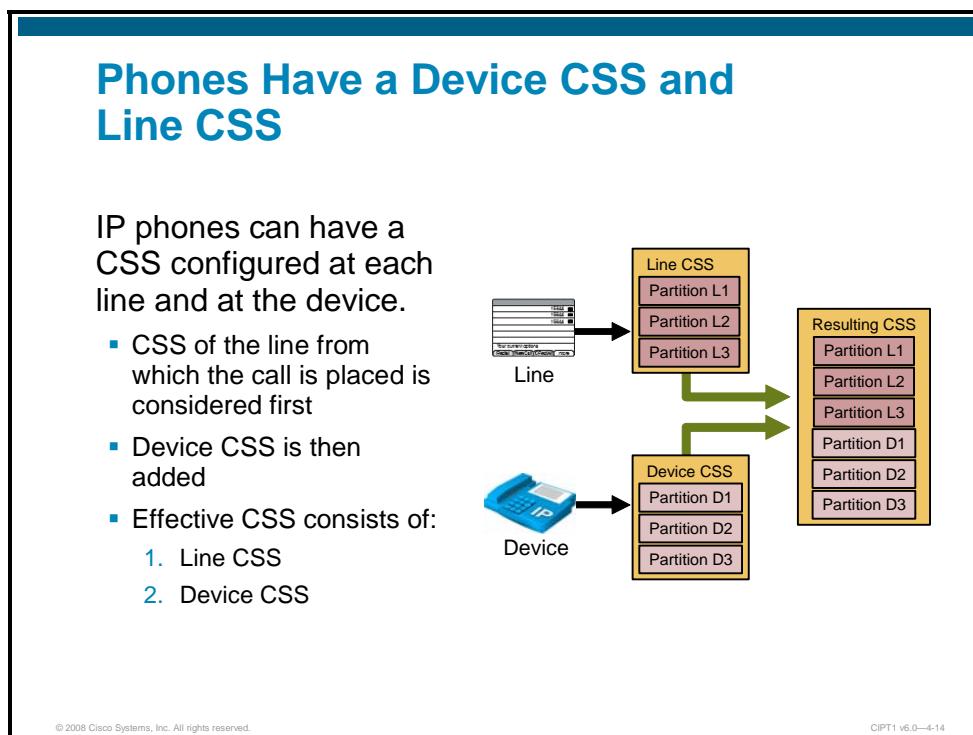
In the example, a user dials 3001 from a phone that has partition Chicago listed as the first partition in its CSS, followed by partition San Jose.

Phone 1-1, Phone 2-1, and Phone 3-1 are all configured with directory number 3001. Phone 1-1 is in partition San Jose, Phone 2-1 is in partition Chicago, and Phone 3-1 is in partition Atlanta.

In this example, Phone 3-1 is not considered for call routing at all, because its partition is not accessible to the calling user (it is not listed in the CSS of the calling phone). From the accessible directory numbers, an equal (full) match is found for two entries: Phone 1-1 and Phone 2-1. Because Phone 2-1 is in the Chicago partition, which is listed first in the CSS of the calling phone, the call is sent to Phone 2-1. If the partitions were listed in reverse order, the call would be sent to Phone 1-1.

Phones Have a Device CSS and Line CSS

This subtopic describes the capability of IP phones to be configured with a device CSS and a line CSS, and how they interact with each other.



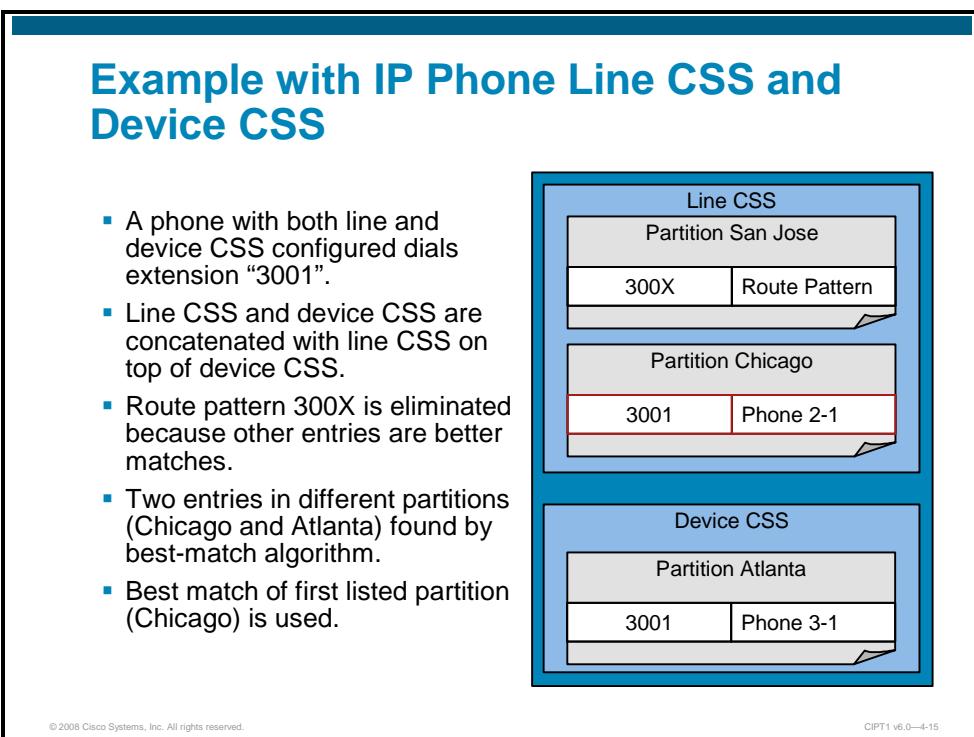
On most sources of a call routing request, such as a trunk, gateway, or translation pattern, only one CSS can be configured. On IP phones, however, a CSS can be applied per line and once at the device level.

If both line and device CSSs are configured, the CSS of the line from which the call is placed is considered first. In other words, the CSS that is used is composed of the partitions listed in the line CSS followed by the partitions of the device CSS.

Note	On computer telephony integration (CTI) ports, the line CSS and the device CSS are placed in reverse order; the partitions of the device CSS are placed before the partitions of the line CSS.
-------------	--

Example with IP Phone Line CSS and Device CSS

The figure provides an example of an IP phone that is configured with a line CSS and a device CSS.



In the example in the figure, the line CSS of the calling phone includes partitions San Jose and Chicago, and the device CSS of the calling phone includes partition Atlanta.

Route pattern 300X is in the San Jose partition, directory number 3001 (used at Phone 2-1) is in the Chicago partition, and the same directory number (3001) is used at Phone 3-1 and assigned with the Atlanta partition.

If the phone dials 3001, the following will happen:

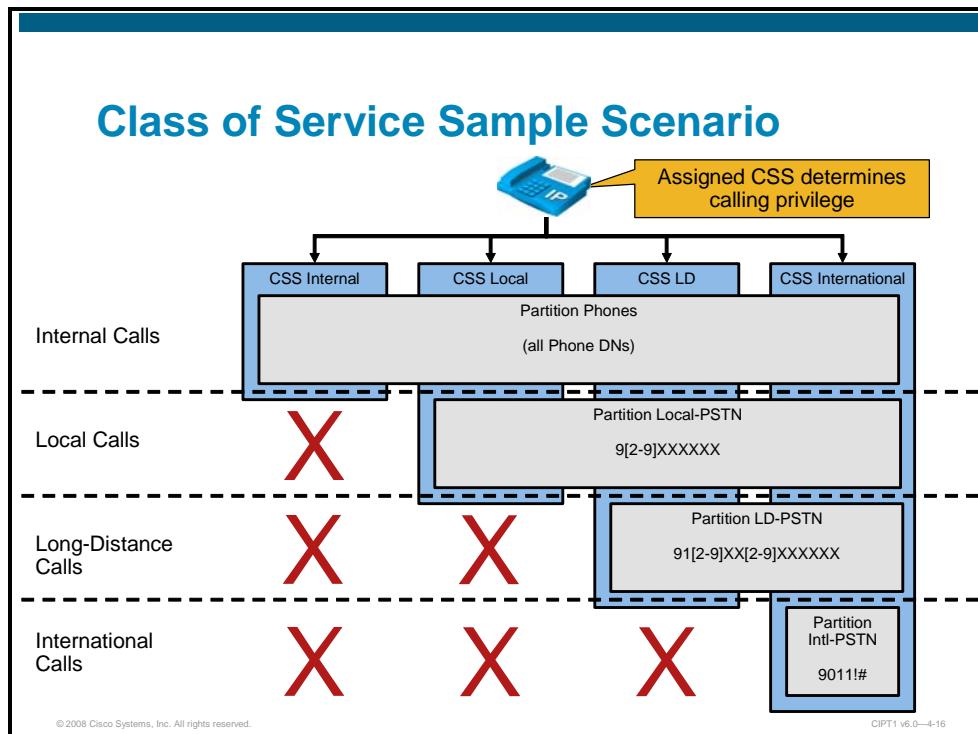
Cisco Unified Communications Manager interprets the dialed digits and searches for the closest match. As the two directory number entries in the call routing table are more specific (full match) than the route pattern (which represents 10 numbers), the route pattern is no candidate for the final routing decision. Out of the two equally matched directory numbers, the one of Phone 2-1 is used to extend the call because it is in the partition that is listed first in the CSS that is effectively used.

This example illustrates that the line CSS has higher priority than the device CSS. If line CSS and device CSS were reversed, the call would be sent to Phone 3-1.

Note	Although route pattern 300X matches the dialed number and is listed in the first partition, it is not used to route the call in this example. This indicates that the first priority for the call routing decision is the best match, and the order of partitions is important only if multiple best matches exist. It is a common misunderstanding that the first matching pattern that is found (regardless of the quality of the match) when searching through the partitions in the order specified in the CSS is used for call routing. If this were true, then subsequent partitions of the CSS would only be looked at if no match was found in the earlier partitions. This is not the case. All partitions are immediately considered for best-match logic, and only if multiple best matches exist is the partition order relevant.
-------------	--

Class of Service Sample Scenario

The figure illustrates an example of implementing class of service in order to limit PSTN calls in different ways.



The example shows the use of partitions and CSS to implement these four different classes of service:

- **Internal Calls:** Allowing internal calls only
- **Local Calls:** Allowing internal calls and local PSTN calls
- **Long-Distance Calls:** Allowing internal calls, local PSTN calls, and long-distance PSTN calls
- **International Calls:** Allowing internal calls, local PSTN calls, long-distance PSTN calls, and international PSTN calls.

The following partitions are created and applied as described:

- **Phones:** This partition is applied to all phone lines.
- **Local-PSTN:** This partition is applied to route pattern 9.[2-9]XXXXXX
- **LD-PSTN:** This partition is applied to route pattern 9.1[2-9]XX[2-9]XX XXXX
- **Intl-PSTN:** This partition is applied to route pattern 9.011!#

The following CSSs are configured, each implementing the corresponding service class:

- **CSS-Internal:** Containing partition Phones
- **CSS-Local:** Containing partitions Phones and Local-PSTN
- **CSS-LD:** Containing partitions Phones, Local-PSTN, and LD-PSTN
- **CSS-International:** Containing partitions Phones, Local PSTN, LD-PSTN, and Intl-PSTN

By applying the appropriate CSS to a phone, the phone is granted the permissions of the respective class of service.

Configuring Partitions and Calling Search Spaces

This subtopic describes how to configure partitions and CSSs and how to apply them to devices or dialable patterns.

Configuring Partitions and Calling Search Spaces

There are two steps of configuration:

- Partition configuration in Cisco Unified CM:
 1. Create new partitions.
 2. Assign partitions to directory numbers, route patterns, translation patterns.
- Calling search spaces configuration in Cisco Unified CM:
 1. Create new calling search space.
 2. Select list of partitions for each calling search space.
 3. Assign calling search space to lines, devices, and translation patterns.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-17

Configuration of partitions and calling search spaces includes the following steps:

- Step 1** Create partitions.
- Step 2** Assign partitions to dialable patterns such as directory numbers, route patterns, or translation patterns.
- Step 3** Create CSSs.
- Step 4** Add partitions in the desired order into each newly created CSS.
- Step 5** Assign CSSs to entities that can request lookups to the call routing table in order to route a call. Examples for such entities are phones and phone lines, trunks, gateways, and translation patterns.

Note	A translation pattern is used in both roles: It is a dialable pattern in the call routing table (that is, the target of a call routing request) and, if matched, it invokes a new call routing request for the translated pattern. The partition at the translation pattern specifies who is able to match the pattern (the partition is required in the CSS of the calling device) and the CSS at the translation pattern specifies the entries of the call routing table that the translation pattern is allowed to see for its call routing request when trying to find the translated pattern in the call routing table.
-------------	--

Creating Partitions

The figure shows how partitions are created in Cisco Unified Communications Manager.

The screenshot shows the 'Partition Configuration' page with the title 'Creating Partitions'. At the top right, there are 'Related Links' for 'Back To Find>List' and 'Go'. A 'Save' button is located at the top left. Below the header, there is a 'Status' section showing 'Status: Ready'. The main area is titled 'Partition Information' with a note about entering multiple partitions, separated by commas. It includes examples like 'CiscoPartition, Cisco employee partition' and 'DallasPartition'. A text input field for 'Name*' contains entries: 'Phones, internal DNs', 'Local-PSTN, local PSTN calls', 'LD-PSTN, long distance PSTN (11 digits)', and 'Intl-PSTN, international PSTN'. A callout box points to this input field with the text 'Enter list of partitions and descriptions (separated by comma)'. At the bottom left is another 'Save' button, and at the bottom right is the text '© 2008 Cisco Systems, Inc. All rights reserved.' and 'CIPT1 v6.0—4-18'.

When adding partitions, Cisco Unified Communications Manager allows all partitions that should be created to be listed in a single input window by specifying the partition name and description in one line, separated by a comma.

Assigning Partitions

The figure shows how to assign partitions to directory numbers and route patterns.

The screenshot displays two side-by-side configuration windows:

- Directory Number Configuration**: Shows a form with fields for Directory Number (1001), Route Partition (Phones), and Active status. The "Route Partition" field is highlighted with a yellow border.
- Route Pattern Configuration**: Shows a form with fields for Route Pattern (9.1[2-9]XX[2-9]XXXXXX), Route Partition (LD-PSTN), and Active status. The "Route Pattern" field is highlighted with a yellow border.

A note box in the center states: "Note: Assign partitions to directory numbers, route patterns, translation patterns, etc."

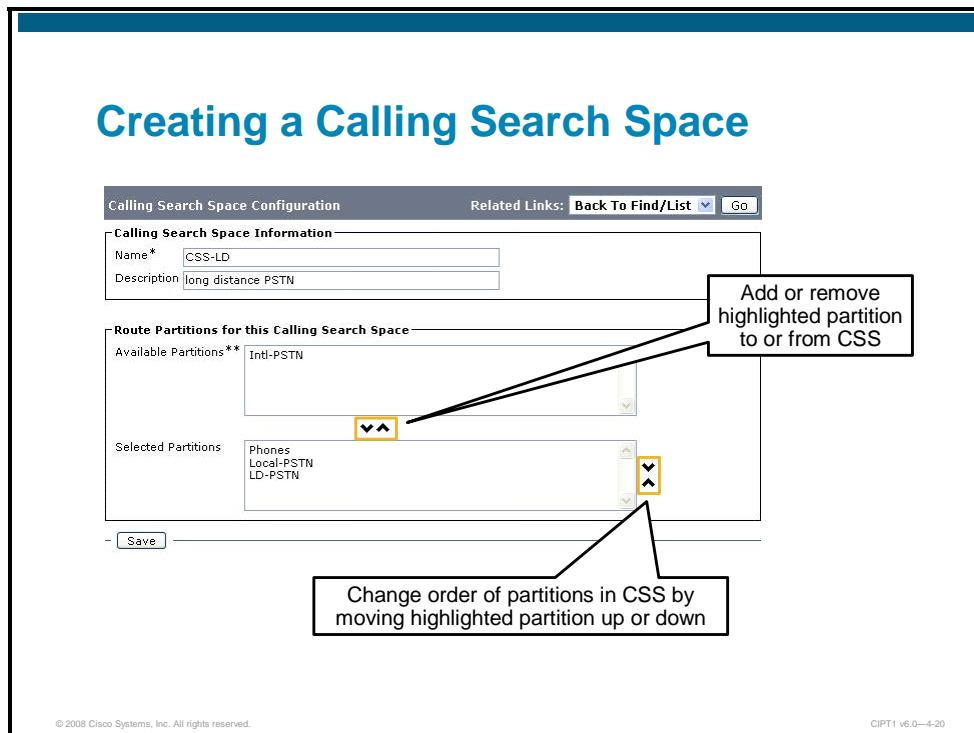
At the bottom left: © 2008 Cisco Systems, Inc. All rights reserved.

At the bottom right: CIPT1 v6.0—4-19

Partitions can be assigned to phone lines (directory numbers), route patterns, translation patterns, or any other call routing target. The figure shows examples for directory numbers and route patterns.

Creating a CSS

The figure shows how to create and configure a CSS.



When adding a CSS, the name, a description (optional), and the ordered list of partitions must be configured.

Note The order of partitions within the CSS is of importance when two equally qualified matches are found. In such a case, the entry of the partition that is listed first is used for the call routing decision.

Assigning a CSS to an IP Phone

The figure shows how to apply a CSS to an IP phone.

The screenshot shows the 'Phone Configuration' screen for a Cisco 7960 IP phone. The 'Device Information' section is displayed, with the 'Calling Search Space' dropdown menu highlighted and set to 'CSS-LD'. A callout bubble labeled 'Assign CSS to Phone' points to this selection. To the right, a note box contains the text: 'Note: Assign CSSs to devices (phones/lines), gateways, translation patterns, etc.' The bottom right corner of the interface shows the version 'CIPT1 v6.0—4-21'.

CSSs can be assigned to phones (as shown in the figure), phone lines, gateways, translation patterns, or any other source of a call routing request.

Time Schedules and Time Periods

This topic describes how to implement time-of-day routing.

Time-of-Day Routing Overview

- Time and date information can be applied to partitions.
- CSSs that include such a partition only have access to the partition if the current date and time match the time and date information applied to the partition.
- Allows different routing based on time
 - Identical route pattern is put into multiple partitions.
 - At least one partition has time information applied.
 - If this partition is listed first in CSSs, it will take precedence over other partition **during the time applied to the partition**.
 - If time does not match, second partition of CSS is used (first one is ignored due to invalid time).

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-23

Time-of-day routing can be implemented in Cisco Unified Communications Manager by applying time and date attributes to partitions using time schedules and time periods. Time periods define time ranges or dates and are grouped into time schedules. Time schedules are then assigned to partitions.

A CSS that includes a partition that is associated with a time schedule only has access to the partition if the current date and time match the date and time information specified in the time schedule that is associated with the partition. If the configured time schedule does not fall into the current date and time, the partition is logically removed from the CSS.

Time-of-day routing can be used to route calls differently based on time in the following way:

- Identical route patterns are created and put into different partitions.
- At least one of these partitions has a time schedule applied.
- If the partition with the time schedule is listed first in CSSs, it will take precedence over other partitions *during the time that is associated with the partition*. If the current time does not match the configured time schedule, the partition that has the time schedule assigned is ignored and the next partition becomes the partition with highest priority.

Time-of-Day Routing Applications

Time-of-day routing can be used for several applications.

Time-of-Day Routing Applications

- Allow international calls only during office hours (based on the time zone of the caller)
- Block international calls on holidays
- Other applications in which you want to control the calling search space based on the time of day:
 - Least cost routing:
 - Multiple providers for international calls
 - Different prices per hours of the day
 - Time-of-day routing allows dialing different providers for same destination (country) based on time

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-24

Some examples of when time-of-day routing can be used are:

- Allowing international calls only during office hours.
- Blocking international calls on holidays.
- Using time-of-day routing to control the call routing path based on the current time, such as the following examples for least-cost routing:
 - Multiple providers for international calls might be available, some of them having different prices depending of the hours of the day (typically more expensive during business hours and less expensive during off-hours).
 - With time-of-day routing, international calls to certain countries can use the cheapest available provider based on the current time, and therefore make use of the cheapest offer for any given time instead of using the same provider for calls to certain countries all of the time.

Time Periods and Time Schedules

This subtopic shows how time periods and time schedules interact with each other.

Time Periods and Time Schedules

Time period	Time Periods	Start–End	Repetition
▪ Time range defined by start and end time	<i>weekdayhrs_TP</i>	0800–1700	M – F
▪ Repetition interval—Days of the week or specified calendar date	<i>weekendhrs_TP</i>	0800–1700	Sat – Sun
▪ Associated with time schedules	<i>newyears_TP</i>	0000–2400	January 1
	<i>noofficehours_TP</i>		Sat – Sun

Time schedule	Time Schedule	Time Periods
	<i>RegEmployees_TS</i>	<i>weekdayhrs_TP</i>

Partition	Time Schedule
<i>CiscoAustin_PT</i>	<i>RegEmployees_TS</i>

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-25

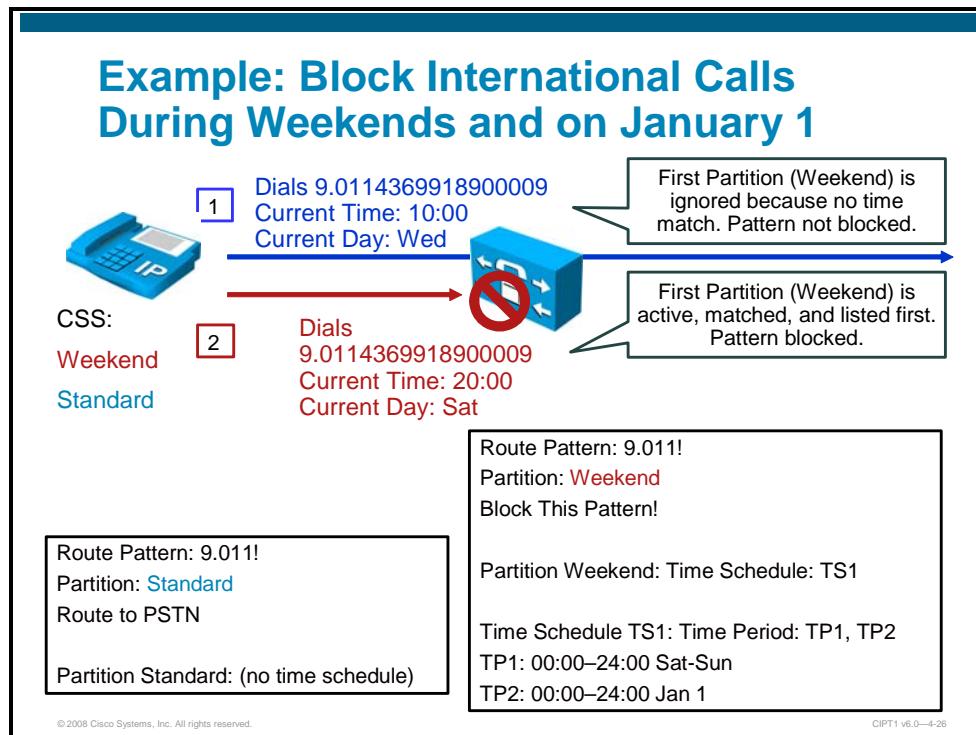
A time period specifies a time range defined by a start and end time and a repetition interval (days of week or specified calendar date). One or more time periods are assigned to a time schedule. The same time period can be assigned to multiple time schedules.

A time schedule is a group of time periods. Time schedules are applied to partitions and thus make the partition inactive in a CSS when the applied time schedule does not match the current date or time.

In the example, partition CiscoAustin_PT is only accessible from Monday to Friday from 0800 hours (8 a.m.) to 1700 hours (5 p.m.) from CSSs that include the partition.

Example: Block International Calls During Weekends and on January 1

The figure shows an example of how international calls can be blocked during weekends and on January 1.



This is implemented by first creating a route pattern which allows international calls. The route pattern is put into the standard partition which has no time schedule applied.

A second, identical route pattern is created which is placed into the Weekend partition.

A time period is configured for Saturday to Sunday 0000 to 2400 hours. Another time period is configured with a specified date: January 1. These two time periods are put into a time schedule and the time schedule is assigned to the Weekend partition.

Phones are assigned with a CSS that contains the Weekend partition first, followed by the Standard partition.

So far, phone users are able to dial international calls at any time because, during weekends and on January 1, they are allowed to dial international based on the Weekend partition, and if that partition is not active (all weekdays except January 1), they are allowed to dial international because of the Standard partition. The task is to configure the route pattern that is in the Weekend partition to be blocked.

Note Route patterns and translation patterns can be configured with the parameter **Block This Pattern** in order to deny the call if the pattern was selected by the call routing logic (best-match, earlier-listed partition).

Now, when the route pattern that is in the Weekend partition is configured to block the call, calls to international are not possible whenever the Weekend partition is active (as listed before the Standard partition in the CSS of the phones). This is the case on weekends and on January 1.

Time-of-Day Routing Configuration Procedure

This subtopic shows how to configure time-of-day routing in Cisco Unified Communications Manager.

Time-of-Day Routing Configuration Procedure

1. Create time periods.
2. Create time schedules.
3. Assign time schedules to partitions.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-27

The steps to implement time-of-day routing are:

- Step 1** Create time periods.
- Step 2** Create time schedules and associate them with time periods.
- Step 3** Assign time schedules to partitions that should be active only during the time specified in the time schedule.

Creating Time Periods

The figure shows an example of time period configuration.

The screenshot displays two separate 'Time Period Configuration' windows side-by-side. Both windows have a header bar with the title 'Creating Time Periods'.

Time Period Configuration (Top Window):

- Time Period Information:**
 - Name*: TP1
 - Time Of Day Start*: 00:00
 - Time Of Day End*: 24:00
 - Repeat Every*: Week from* Sat through* Sun
 - Year on* None
- Buttons:** Save

Time Period Configuration (Bottom Window):

- Time Period Information:**
 - Name*: TP2
 - Time Of Day Start*: 00:00
 - Time Of Day End*: 24:00
 - Repeat Every*: Week from* None through* None
 - Year on* Jan 1
- Buttons:** Save

Annotations:

- A callout box points to the 'Repeat Every' section of the TP1 configuration, stating: "TP1 is active Saturday and Sunday from 00:00 to 24:00".
- A callout box points to the 'Repeat Every' section of the TP2 configuration, stating: "TP2 is active Jan 1 from 00:00 to 24:00".

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—4-28

When creating time periods, a name, a time of day start and end time, and a repetition interval must be configured. The repetition interval can be a range of weekdays or a date of the year.

In the example, two time periods are created, TP1 is active from Saturday to Sunday, 00:00 to 24:00, and TP2 is active on January 1 of each year.

Creating Time Schedules

The figure shows an example of time schedule configuration.

Creating Time Schedules

Time Schedule Configuration

Status
(i) Status: Ready

Time Schedule Information
Name* TS1

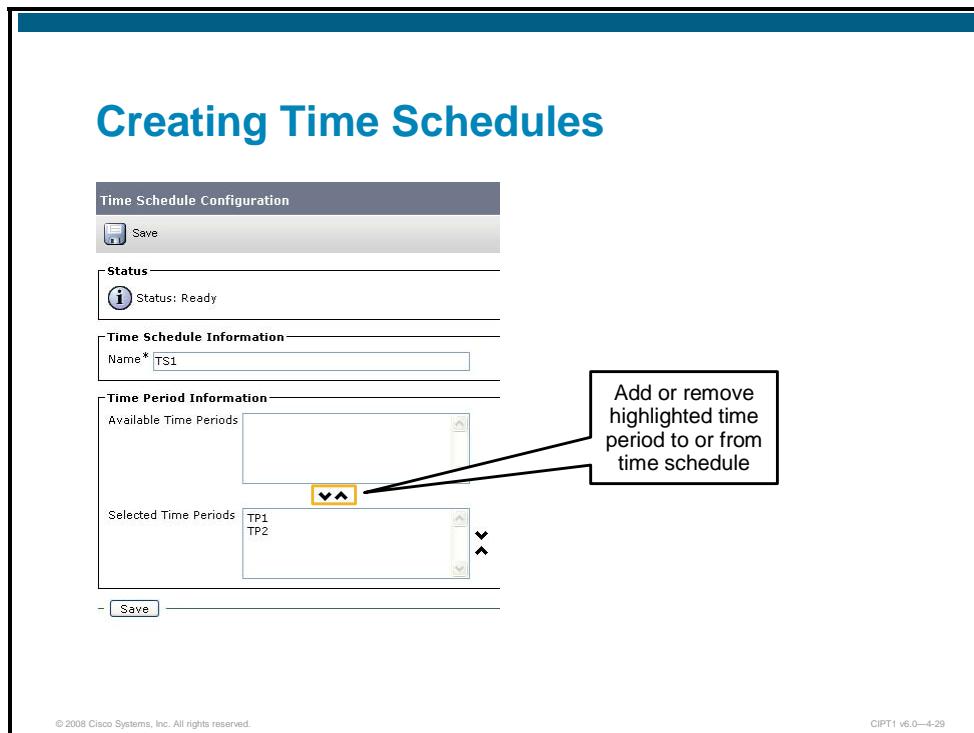
Time Period Information

Available Time Periods

Selected Time Periods TP1 TP2

Add or remove highlighted time period to or from time schedule

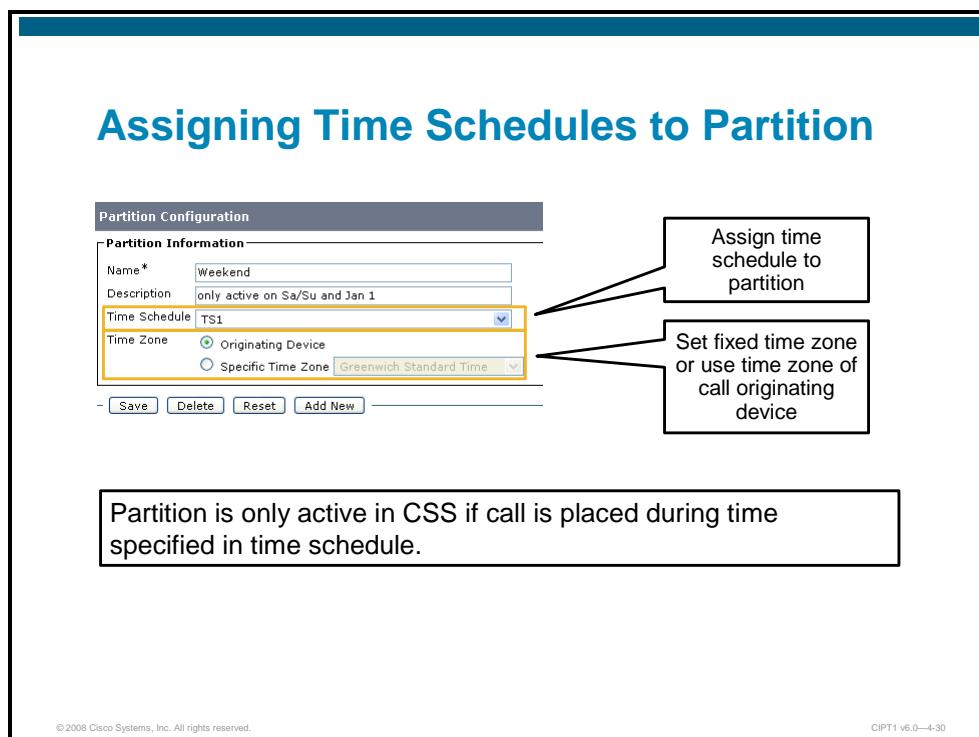
© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—4-29



When creating a time schedule, a name and a list of time periods must be configured.

Assigning Time Schedules to Partition

The figure shows how to assign time schedules to partitions.



Time schedules can be assigned to partitions. In the example, the earlier configured time schedule, TS1, is applied to partition Weekend. As a result, partition Weekend is only active in CSSs if a call is placed during the time specified in the time schedule.

Note

The configuration screenshots refer to the example provided earlier in which the partition Weekend is assigned to a route pattern (9.011!), which is configured to block the call. The same route pattern also exists in another partition (Standard), in which the call is sent toward the PSTN. In the phone CSSs, partition Weekend is listed *before* partition Standard. This is important to ensure that partition Weekend is used if it is active. As partition Weekend is only active on Saturdays, Sundays, and on January 1, the blocked route pattern will be matched on these days. On all other days, the route pattern in partition Standard is matched (which is now the only active partition in the CSS) and the call is sent to the PSTN.

Understanding CMC and FAC

This topic describes Client Matter Codes and Forced Authorization Codes.

Client Matter Codes and Forced Authorization Codes

- CMC: Forces the user to enter any configured CMC
 - Allows for billing and tracking of calls made per client
- FAC: Forces the user to enter a configured authorization code with a high-enough authorization level
 - Prevents unauthorized user from making toll calls
 - Can be combined with time-of-day routing (e.g., international calls outside business hours require FAC)
- Both generate Call Detail Records



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-32

CMC and FAC can be applied to route patterns.

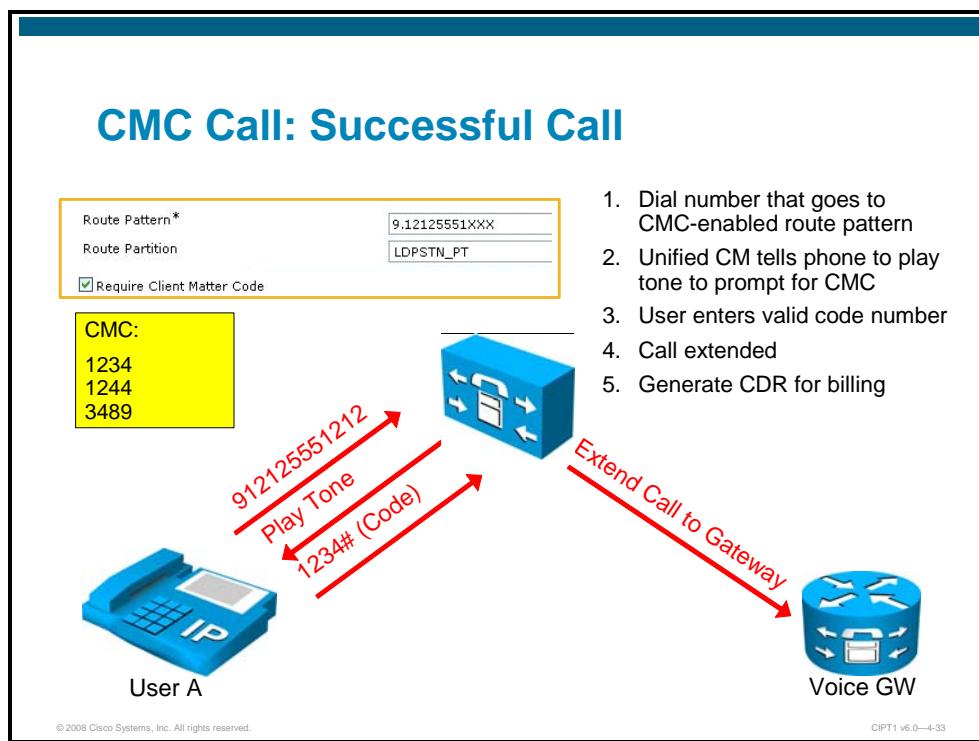
If a route pattern that has a CMC applied is matched, the user is prompted to enter a CMC for the call to be extended. The CMC is added to Call Detail Records in order to allow accounting and billing of calls based on their client matter.

If a route pattern is matched to a pattern which has an FAC applied, the user is prompted to enter an FAC for the call to be extended. The idea of FACs is to prevent calls to be placed from unauthorized users, or, in other words, to only allow FAC-protected patterns to be used from users who are authorized to use the pattern (by knowing a corresponding FAC).

Valid CMCs and FACs are added to Cisco Unified Communications Manager and an authorization level is assigned to FACs. If an FAC is required for a route pattern, the minimum required authorization level has to be specified at the route pattern. In order for calls to be extended, users must enter any valid CMC to pass CMC prompts, and users must enter a valid authorization code whose authorization level is equal or greater than the level configured at the FAC-enabled router pattern.

CMC Call: Successful Call

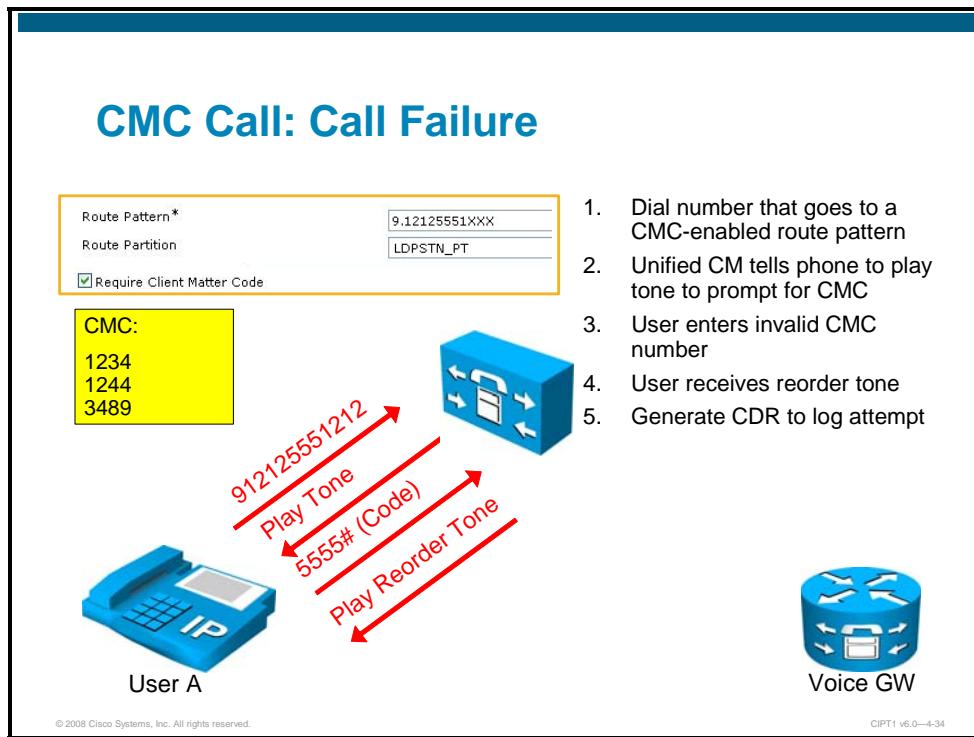
The figure illustrates a successful call when dialing a CMC-enabled route pattern.



User A dials a number which matches a route pattern where the Require Client Matter Code parameter is checked. Cisco Unified Communications Manager plays a tone to indicate to the user that a CMC must be entered. The user has to enter any valid CMC for the call to be extended. In the example, CMC 1234, 1244, and 3489 are configured and the user enters 1234. The call is successful and the entered CMC is included in the generated Call Detail Record (CDR).

CMC Call: Call Failure

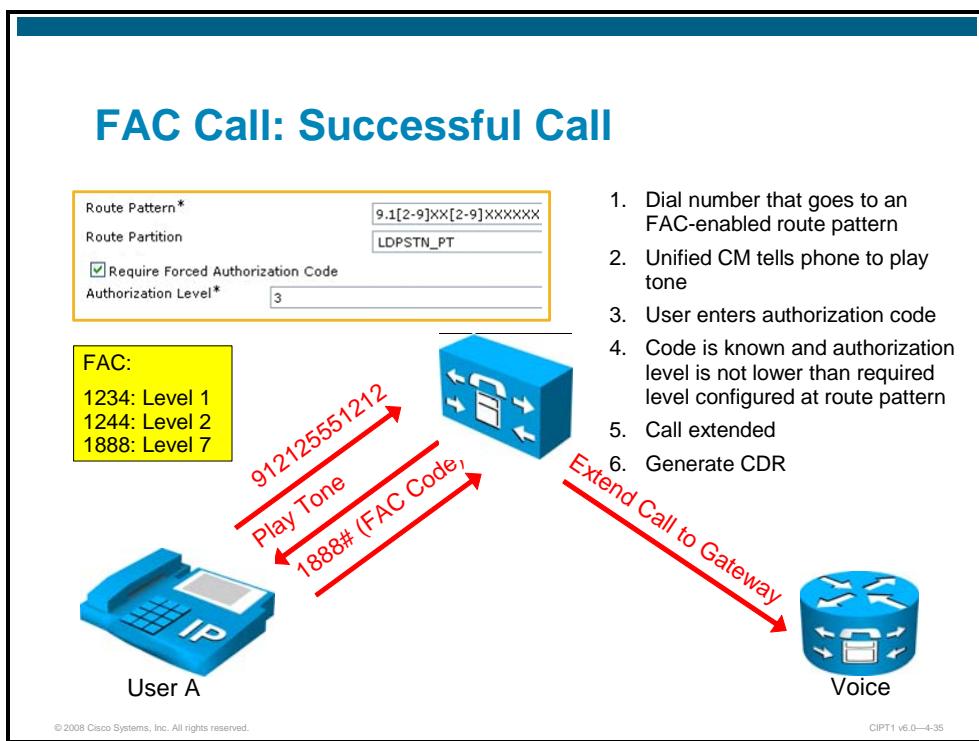
The figure illustrates a call failure when dialing a CMC-enabled route pattern.



The configuration is the same that was used in the previous example, but this time User A enters 5555 at the CMC prompt. This is not a valid CMC and therefore the call is denied. A CDR is generated logging the attempted call.

FAC Call: Successful Call

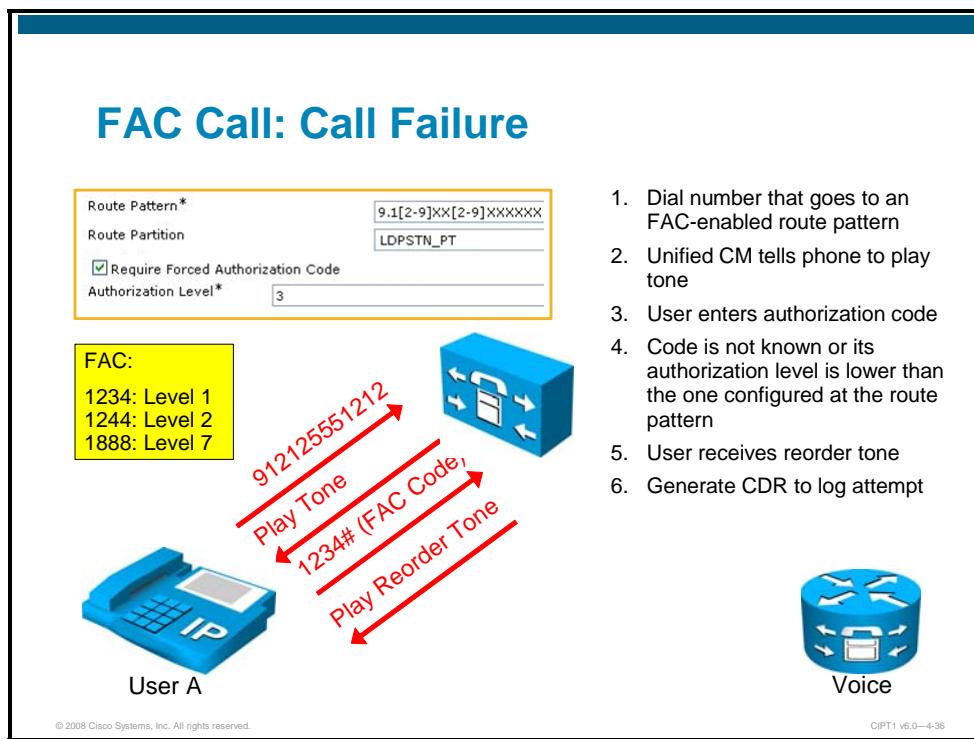
The figure illustrates a successful call when dialing an FAC-enabled route pattern.



User A dials a number that matches a route pattern, where the Require Forced Authorization Code parameter is checked and the Authorization Level is set to 3. Cisco Unified Communications Manager plays a tone to indicate to the user that an FAC must be entered. The user must enter a valid FAC with an authorization level of 3 or above for the call to be extended. In the example, FAC 1234 is configured with a level of 1, FAC 1244 is configured with a level of 2, and FAC 1888 is configured with a level of 7. At the prompt, the user enters 1888. The call is successful and the name of the entered FAC is included in the generated CDR.

FAC Call: Call Failure

The figure illustrates a successful call when dialing an FAC-enabled route pattern.



The configuration is the same as that used in the previous example, but this time User A enters 1234 at the FAC prompt. Although this is a valid FAC, the call is denied because the authorization level of the entered FAC (level 1) is lower than the required level configured at the route pattern. A CDR is generated logging the attempted call.

Calling Privileges Applications Overview

This topic describes applications for partitions and calling search spaces, and other calling privileges configuration elements.

Different Ways Of Using Calling Privileges Configuration Tools

Partitions and CSS are primarily used to implement class of service.

- Primarily used to implement class of service when you must to **permit or deny** access to a **certain number**
 - International versus long distance versus local
 - Direct access to managers versus going through assistant
 - Can include time of day or require an authorization code
- Configuration tools can also be used for applications such as these.
 - Vanity numbers: **depending on who is calling** a number, the call is **routed differently**
 - Time of day-based path selection: **depending on time** a number is called, call is **routed differently**
 - Private line, automatic ringdown (PLAR): automatically **dial one specific number** when phone goes **off-hook**

© 2008 Cisco Systems, Inc. All rights reserved.

CPT1 v6.0—4-38

Calling privileges configuration elements are primarily used to implement class of service when you must permit or deny access to certain destinations depending on the caller. Examples include different classes of service for PSTN access (international dialing versus long-distance calls versus local calls), direct access to managers versus being transferred by assistants, permissions based on time of day or depending on successfully providing authorization codes, and so on.

However, the same configuration tools can be used to implement other applications, typically those in which calls are not permitted or denied but routed in a different way depending on who is placing the call. Examples include vanity numbers and emergency dialing, time of day-based carrier selection for PSTN calls, or PLAR.

Note	PLAR makes a phone dial a specific preconfigured number as soon the phone goes off-hook.
-------------	--

Calling Privileges Application Examples

The table lists calling privileges applications and descriptions.

Calling Privileges Application Examples	
Applications	Description
Class of service: Limiting access to certain destinations	Traditional calling privileges; who is allowed to call where or whom.
911 emergency calls and vanity numbers	All users dial the same number, but depending on the caller, the call goes to a different destination.
Time of day-based carrier selection	Time-of-day routing is used to select different carriers based on the time of the day.
Mandatory call accounting	Calls must be flagged: Business versus private calls, client-based call accounting and billing, etc.
PLAR	Going off-hook connects the phone to a specific destination; user cannot dial.

© 2008 Cisco Systems, Inc. All rights reserved.

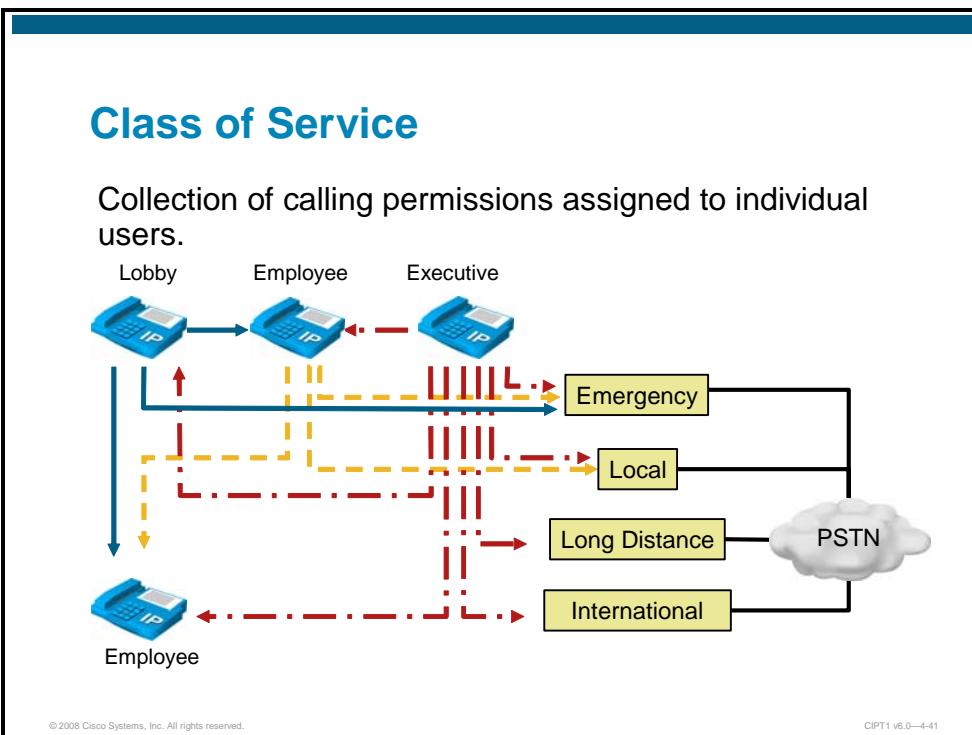
CIPT1 v6.0—4-39

Each application listed in the table has different requirements regarding the configuration tools or elements that are needed for implementing the application. The requirements are as follows:

- **Class of service:** Limiting access to certain destinations. Partitions and CSSs, time schedules and time periods, blocked patterns, CMC, and FAC (listed in descending popularity) are typically used to implement class of service.
- **911 emergency calls and vanity numbers:** Partitions and CSSs are typically used to implement vanity numbers and emergency dialing.
- **Time of day-based carrier selection:** Partitions and CSS, time schedules and time periods are typically used for this application.
- **Mandatory call accounting:** CMC are typically used to extend calls only if they are flagged with accounting information.
- **PLAR:** Translation patterns, partitions, and CSSs are typically used to implement PLAR.

Implementing CoS

This topic describes how to implement CoS in Cisco Unified Communications Manager.



Class of service is the collection of calling permissions that are assigned to individual users.
Class of service can be implemented in different ways.

Implementing CoS: Traditional Approach

This subtopic describes the traditional approach to implementing CoS.

Implementing CoS: Traditional Approach

- Place external route patterns in partitions associated with the destinations that they can call
- Configure each calling search space to be able to reach only the partitions associated with its call restriction policy
- Assign these calling search spaces to the phones by configuring them on the Unified CM device pages (all lines on the device automatically receive the same CoS)

© 2008 Cisco Systems, Inc. All rights reserved.

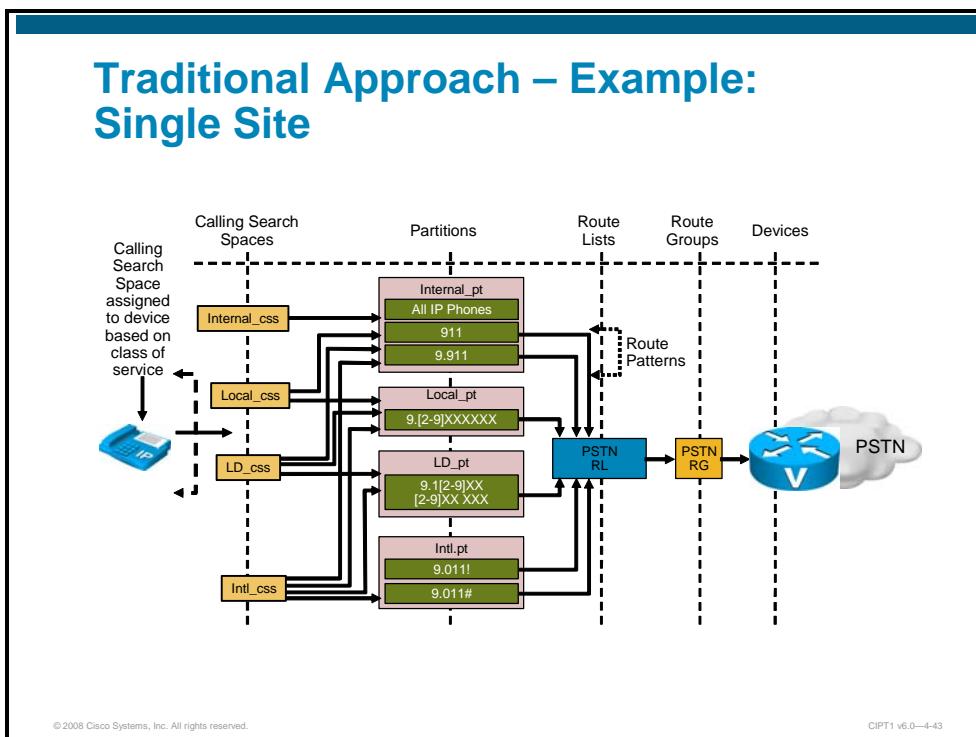
CIPT1 v6.0—4-42

When using the traditional approach of CoS implementation in Cisco Unified Communications Manager, external route patterns are placed into partitions. CSSs are configured per class of service and applied to the respective phones. No CSSs are applied to lines and therefore the phone CSS applies to all lines.

It may sound reasonable not to use the separate line CSS, because typically a phone should have the same privileges on all its lines.

Traditional Approach – Example: Single Site

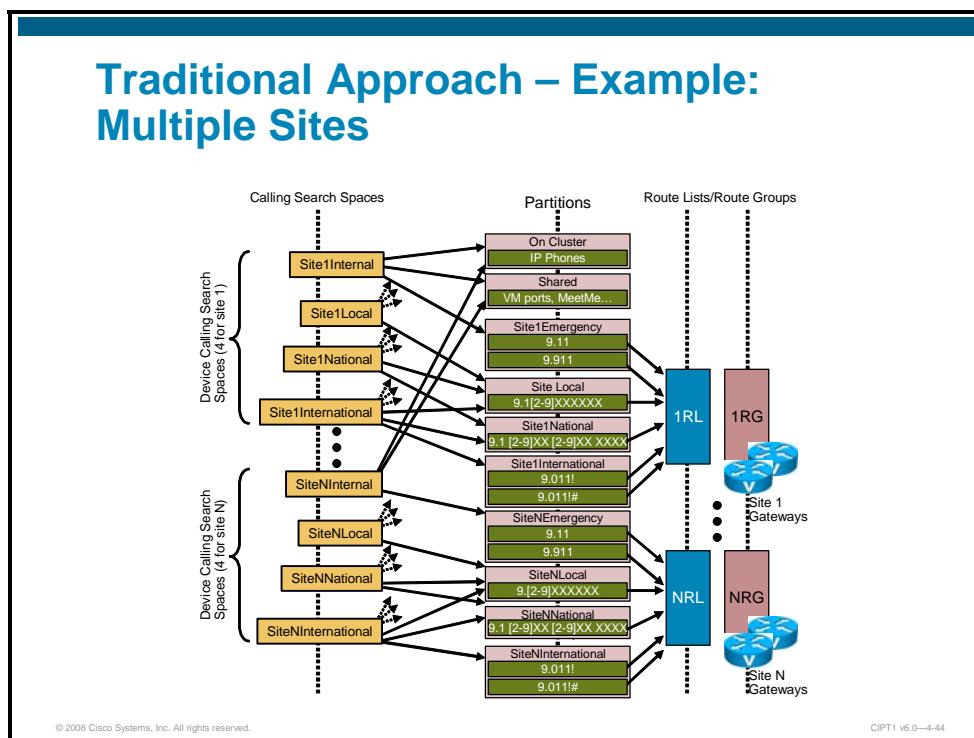
The figure shows an example of using the traditional approach for implementing CoS in a single-site deployment.



The traditional approach has no problems or disadvantages as long as it is used in a single-site environment in which all devices should use the same PSTN gateway for external route patterns. Such a scenario is shown in the example in the figure.

Traditional Approach – Example: Multiple Sites

The figure shows how complexity increases when using the traditional approach in multisite environments.



The problem in multisite environments is that partitions and CSSs need to provide two functions: First, they must select the local PSTN gateway for each individual site, and, secondly, they must control who is allowed to dial what number.

The selective PSTN breakout is achieved by creating all PSTN route patterns once per gateway—always in a different, site-specific partition. In addition, all these route patterns must be duplicated, varying the partition by a class of service-specific tag, so that headquarters users with different CoS can have a CSS that includes a partition providing access to a certain CoS and their local gateway.

In the figure, this can be observed by looking at the partitions that include PSTN targets. There is a Site1Emergency partition, a Site1National partition, a Site1International partition (providing three different CoS to Site1 users), and the same three CoS partitions must exist for each additional site (SiteNEmergency, SiteNNational, and SiteNInternational). The number of required partitions is calculated by multiplying the number of required classes of service by the number of sites. This does not scale to large deployments.

Line Device Approach: Improves Scalability

In order to improve scalability of CoS implementation in multisite environments, you can use a line device approach.

Line Device Approach: Improves Scalability

Significantly decreases the total number of partitions and CSS required.

- Use the device calling search space to provide call routing information (for example, which gateway to select for **all** PSTN calls).
- Use the line calling search space to provide class of service information (for example, which of the PSTN calls to block).

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-45

The traditional approach to implementing CoS in a multisite environment can result in a large number of partitions and CSSs when applied to large multisite deployments with centralized call processing. This configuration is required because the device CSS is used to determine both the path selection (that is, which PSTN gateway to use for external calls) and the CoS.

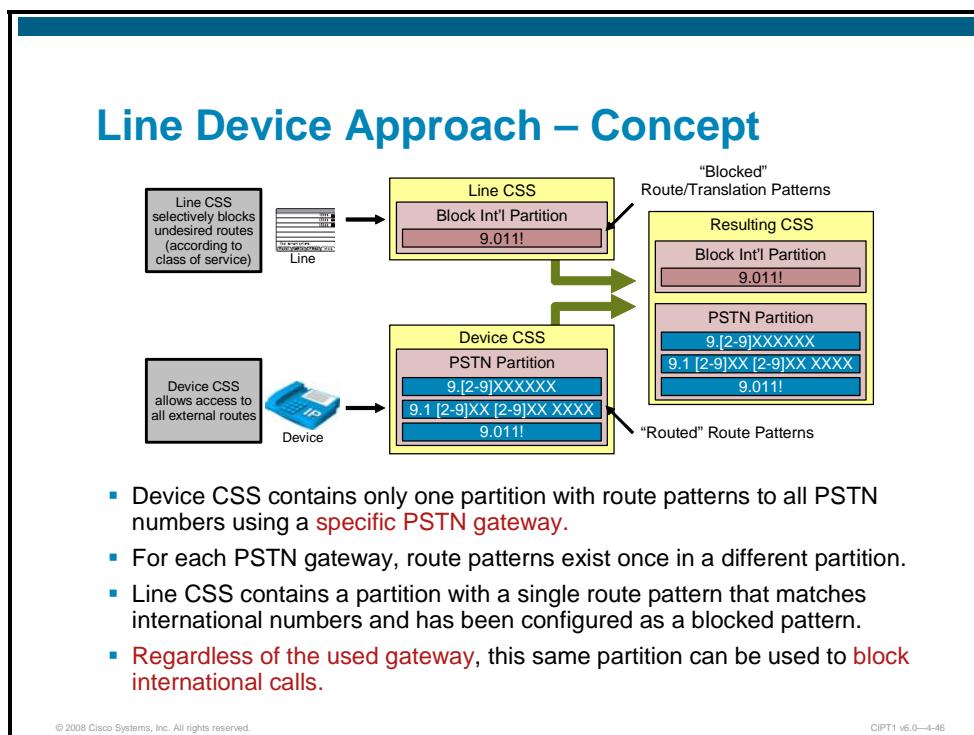
You can significantly decrease the total number of partitions and CSSs needed by dividing these two functions between the line CSS and the device CSS, which is called the line device approach.

Based on the way in which the line CSS and the device CSS for each given IP phone are combined, follow these rules to implement the line device approach:

- Use the device CSS to provide call routing information (for example, which gateway to select for **all** PSTN calls).
- Use the line CSS to block route patterns that are not allowed by certain CoS (independent of the used PSTN gateway).

Using a Line Device Approach

The figure shows how the line device approach works in Cisco Unified Communications Manager.

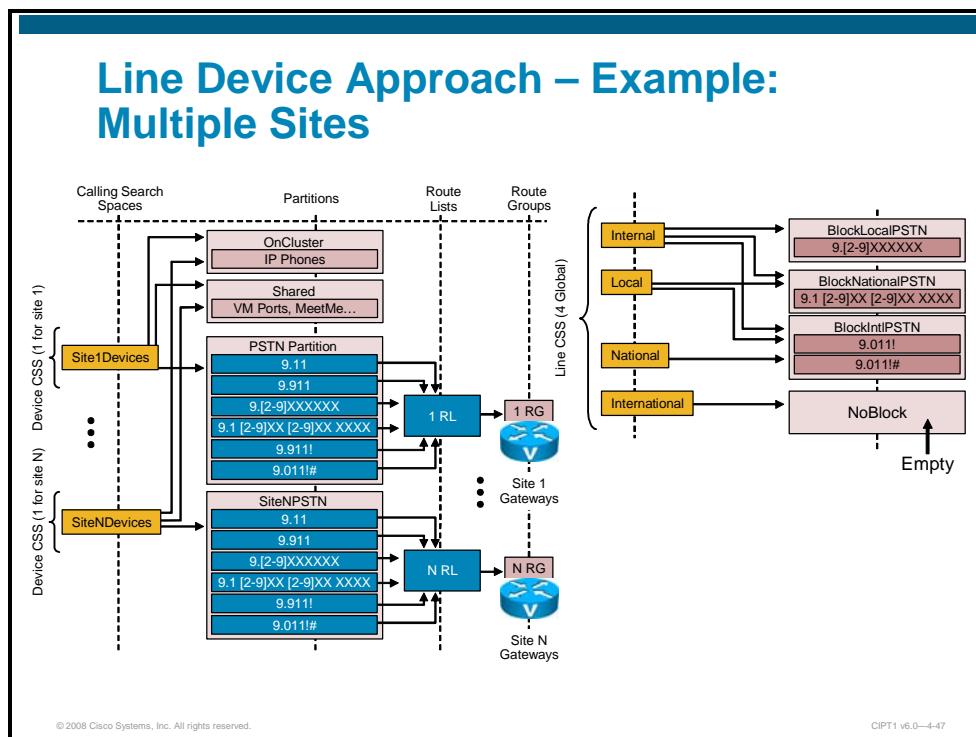


Create an unrestricted CSS for each site and assign it to the phone device CSS. This CSS should contain a partition featuring route patterns that route the calls to the appropriate local gateway per site.

Create CSSs containing partitions with blocked route patterns for those types of calls not permitted by the CoS of a user, and assign them to the lines of the user phone. For instance, if a user has access to all types of calls except international, that user line (or lines) should be configured with a CSS whose first partition includes a route pattern that blocks calls to 9.011!.

Line Device Approach – Example: Multiple Sites

The figure shows an example of using the line device approach for implementing CoS in a multisite deployment.



In the example in the figure, the line device approach is used, resulting in a significantly simpler configuration.

One partition is used per CoS to block destinations that are not desired by the appropriate CoS. These partitions are included in the line CSS of the device in order to always block access to destinations which are not permitted for the corresponding CoS, regardless of the PSTN gateway that is going to be used by devices of a certain location.

In addition, all possible PSTN route patterns are created once per PSTN gateway and put into a partition that is included at the device CSS, thus allowing the local gateway to be used for all PSTN calls that have not been blocked earlier by the line CSS.

This approach has the significant advantage that only a single, site-specific partition (and device CSS) is required for each site in order to allow local gateway selection, and only one partition per CoS (independent of the site) is required in addition.

Rather than requiring a number of partitions calculated by multiplying CoS and sites, the number of partitions is determined by adding the required sites and classes of service.

For example, with 4 sites and 4 classes of service, using the traditional approach, 16 partitions are required, while using the line device approach, the number of partitions drops to 8.

Implementing 911 and Vanity Numbers

This topic describes how to implement vanity numbers and emergency dialing.

911 Emergency Number

911 is a single number to call for medical, fire, and police emergencies, legislated in Canada and United States:

- Calls to 911 are routed to a PSAP. The PSAP is the first-tier triage call center for emergency calls.
- 911 calls must always be sent to the local PSAP .
- Calls to the same number must be routed differently per phone (location).

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-49

911 is a single number to call for medical, fire, and police emergencies in the U.S. and Canada. Calls to 911 are routed to a public safety answering point (PSAP). The PSAP is the first-tier triage call center for emergency calls. PSAP operators dispatch or conference medical, fire, and police resources as necessary.

Emergency calls have to be sent to a local PSAP through the local gateway. In a multisite environment, this means that emergency calls placed to the same number must be routed differently depending on the physical location of the calling phone. The same method is usually applied to all PSTN destinations in order to keep voice traffic off the IP WAN and keep local gateways free in the event of a PSTN outbreak.

Note	Emergency calling in the U.S. and Canada includes additional aspects that are not covered in this course.
-------------	---

Vanity Numbers

This subtopic describes the characteristics of vanity numbers.

Vanity Numbers

- Vanity numbers provide a certain **local service**
- Same number regardless of your physical location
- Examples:
 - Dial 7999 at any site to get local IT support (on-net)
 - Dial 7998 at any site to get local travel agency (off-net)
- Number can be a route pattern, directory number, or hunt pilot
- 911 emergency dialing has the same basic concept
 - Dial 911 at any site to get to local emergency services (off-net, emergency call)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-50

Vanity numbers provide access to a certain local service within an enterprise. Users should be able to dial the same number to access the appropriate locally provided service no matter where they are located.

An example could be a number, for example, 7999, that always connects users to the local IT support. Vanity numbers are not limited to internal services, such as the IT support example, but could also be configured to reach external local services such as taxi or travel agencies by using abbreviated dialing (for example, 7998).

The vanity number can be a directory number, a route pattern, a hunt pilot, or a translation pattern.

Note

More information about call hunting is provided in the next lesson of this module.

Implementing Emergency and Vanity Numbers in Cisco Unified Communications Manager

This subtopic describes how to implement vanity numbers in Cisco Unified Communications Manager.

Implementing Emergency and Vanity Numbers in Unified CM

- Create a site-specific partition for each physical location.
- For each service, configure the same vanity number (route pattern or directory number or hunt pilot) once per physical location and apply respective site-specific partition.
- Put the appropriate site-specific partition into the CSS of phones.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-51

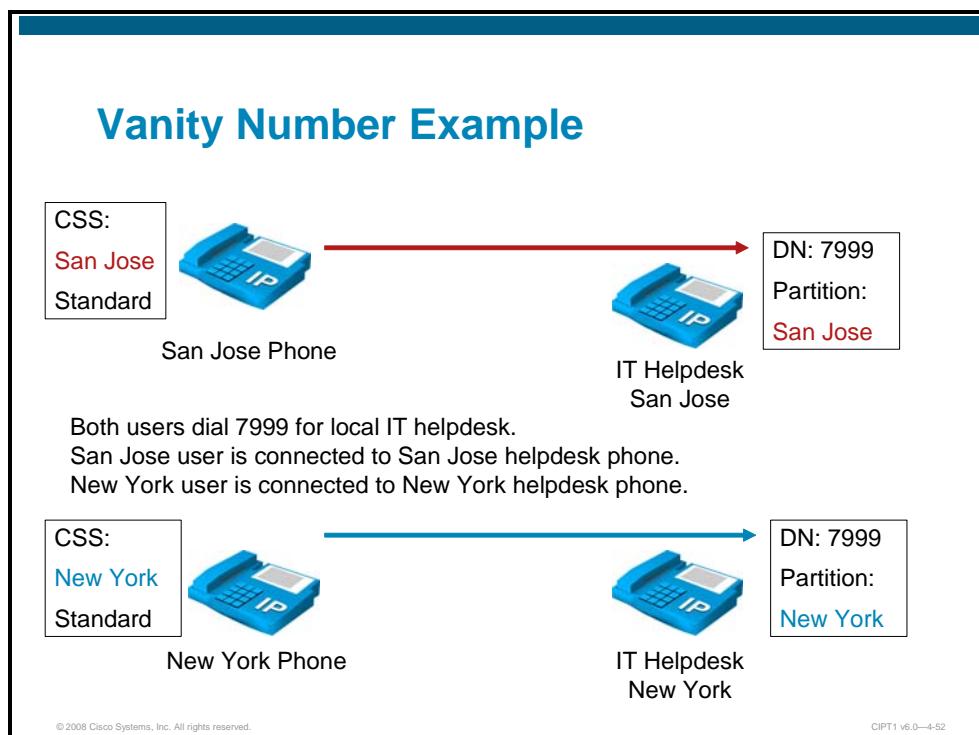
The way to implement vanity numbers is similar to configuring selective PSTN outbreak (always using the local gateway for PSTN or emergency calls):

- Step 1** Create a site-specific partition per site.
- Step 2** For each service, configure the same vanity number (route pattern, directory number, hunt pilot, or translation pattern) once per site and put it into the site-specific partition created earlier.
- Step 3** Put the appropriate site-specific partition into the CSS of the phones located at a site.

Note If abbreviated dialing is used to reach external local services (such as a local travel agency, by dialing 7998) a translation pattern will be used for the vanity number.

Vanity Number Example

The figure shows an example of vanity number implementation in Cisco Unified Communications Manager.



In the example in the figure, the vanity number for IT support is 7999. There are two sites: New York and San Jose. The directory number 7999, located in San Jose, is put into the San Jose partition, and the same directory number located in New York is put into the New York partition. Phones located in New York have the partition New York listed first in their CSS; phones located in San Jose have the partition San Jose listed first in their CSS.

If a San Jose user dials 7999, the call is routed to the IT helpdesk phone. The New York directory number 7999 is not accessible by the San Jose phone because the phone CSS does not include partition New York. The same applies vice versa to users in New York.

Additional Example:

If the desired service were provided externally, a translation pattern could be configured to translate the appropriate vanity number (for example, 7998 to access a local travel agency) to the site-specific PSTN number. By creating the vanity number once per site and putting it into a site-specific partition, it can ensure that users always match the vanity number translation pattern for their respective site. This is achieved by including the site-specific partition in the phone CSS. In the above example, the only changes would be as follows:

Use two translation patterns 7998 instead of two directory numbers 7999. As with the directory numbers, put them into site-specific partitions (San Jose and New York). Configure the San Jose translation pattern with the PSTN number of the San Jose travel agency; configure the New York translation pattern with the PSTN number of the New York travel agency. Make sure that the translation patterns have CSSs assigned that allow them to use the local PSTN gateway for routing calls out to the translated PSTN numbers.

Implementing Time of Day-Based Carrier Selection

This topic describes how to implement time of day-based carrier selection for international or long-distance calls.

Implementing Time of Day-Based Carrier Selection

Different approaches depending on scenario:

- Dedicated gateway per carrier
 - Configure required route patterns (international, long distance, local, etc.) once per carrier pointing to appropriate carrier gateway; put route patterns into a carrier-specific partition
 - Apply time-of-day settings to each partition and include all partitions in CSS of phones
- Single PSTN access with carrier access code (1010) and 3-digit carrier identification code
 - Configure route patterns; once per carrier and transform dialed number to include carrier access and carrier identification codes; put them into a carrier-specific partition
 - Apply time-of-day settings to each partition and include all partitions in CSS of phones

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-54

Depending on the way that the long distance or international carrier is selected, there are the following two approaches for implementing time of day-based carrier selection:

■ Dedicated gateway per carrier

Follow these steps to create a dedicated gateway per carrier:

- Step 1** Configure required route patterns (patterns that should be routed differently based on the time of day) once per carrier, pointing to the appropriate carrier gateway.
- Step 2** Put the route pattern into a carrier-specific partition.
- Step 3** Apply time-of-day attributes to each partition.
- Step 4** Include all carrier-specific partitions in phone CSSs.

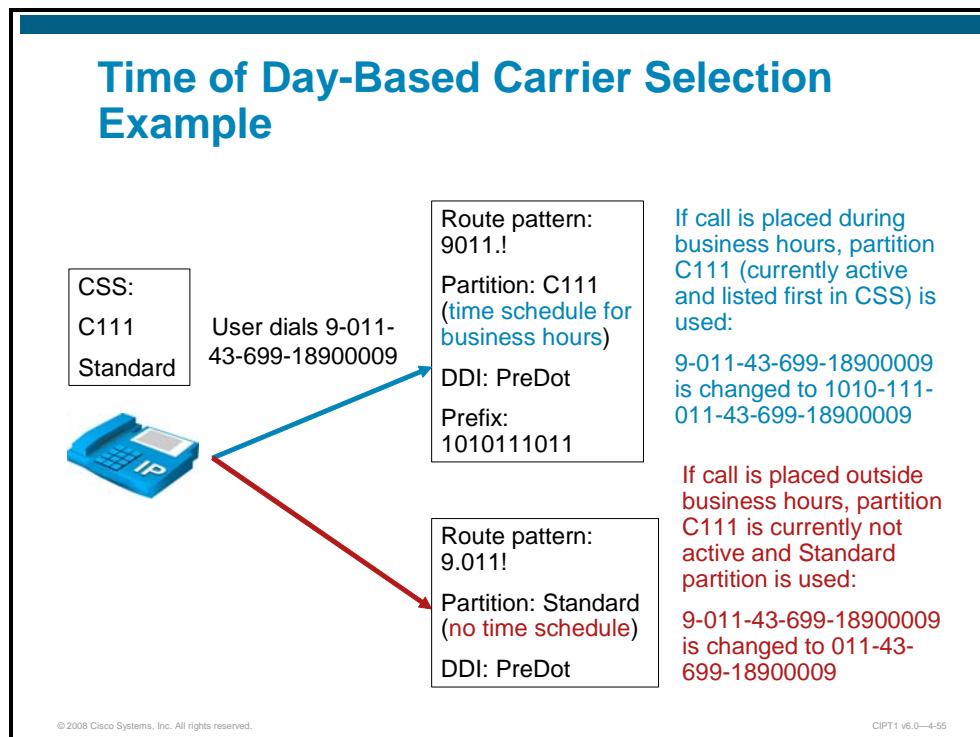
■ Single PSTN access with carrier access code (1010) and 3-digit carrier identification code

Follow these steps to create single PSTN access:

- Step 1** Configure required route patterns (patterns that should be routed differently based on the time of day) once per carrier and transform the dialed number to include carrier access and appropriate carrier identification code.
- Step 2** Put the route pattern into a carrier-specific partition.
- Step 3** Apply time-of-day attributes to each partition.
- Step 4** Include all carrier-specific partitions in phone CSSs.

Time of Day-Based Carrier Selection Example

The figure shows an example of implementing time of day-based carrier selection.



In the example in the figure, two route patterns are configured for international calls. One is in partition C111 (indicating that it is using the carrier with ID code 111) and the other is in no partition.

The carrier with ID 111 is cheaper for international calls during business hours; in all other situations (other PSTN destinations or international calls placed outside business hours), the standard PSTN provider should be used.

The route pattern that is in partition C111 is set up as 9011.! in order to allow the 9011 to be stripped off (by PreDot discard digit instructions [DDI]). In addition, a prefix 1010-111-011- is configured. As a result, after stripping off 9011 and adding 1010-111-011- to the number, it results in a call with carrier access enabled (1010) using the carrier with the ID 111 followed by the international number (011) (country code 43, area code and subscriber number 69918900009).

The other route pattern (9.011!) is configured with PreDot DDI, which only strips off the access code 9, resulting in a standard international call number (011 followed by the international number).

Now, when the digit manipulation is set up correctly for both situations—matching the 9011.! route pattern, which is in the C111 partition, and matching the 9.011! route pattern, which is in no partition—the only problem remaining is that the pattern in partition C111 is preferred over the other pattern during business hours. This can be easily fixed by applying a corresponding time schedule to the partition and including the partition in the phone CSS.

Implementing PLAR

This topic describes how to implement PLAR in Cisco Unified Communications Manager.

Implementing PLAR

Use PLAR to make a phone dial a predefined number when the phone goes off-hook.

- Implemented by using partitions, CSS, and translation patterns
 - Translation pattern with a null-string pattern is created and put into a partition
 - Dialed number (null-string) is transformed to PLAR destination number
 - Partition is the only entry in CSS of phone
 - Translation pattern requires access to PLAR destination (CSS with partition of PLAR destination or no partition at PLAR destination)
- When phone goes off-hook, the dialed string (null string to indicate off-hook status) matches the translation pattern and is translated to PLAR number

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-57

PLAR is used when a phone should dial a predefined number when the phone goes off-hook.

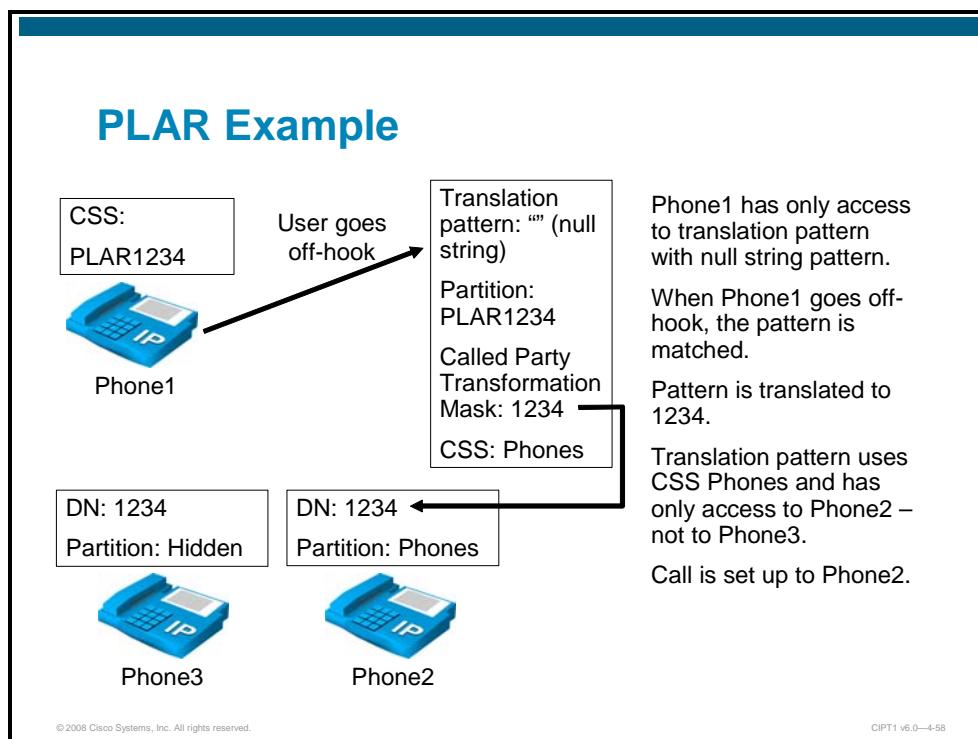
Follow these steps to implement PLAR in Cisco Unified Communications Manager:

- Step 1** Configure a translation pattern in which the pattern is empty (null string pattern) and put it into a partition.
- Step 2** Configure the number to be dialed by the PLAR-enabled phone in the called party transformation mask of the translation pattern.
- Step 3** Configure the phone that should use PLAR with a CSS that only includes the partition that was applied to the translation pattern.
- Step 4** Make sure that the translation pattern has access to the transformed number (that is, the PLAR destination) because the translation pattern CSS is used when making the call routing decision for the translated number.

When the phone goes off-hook, the dialed string (null string to indicate the off-hook status is sent to Cisco Unified Communications Manager) matches the translation pattern and is translated to the PLAR number. The call is then extended towards the PLAR destination.

PLAR Example

The figure shows a sample configuration for a phone configured for PLAR.



In the example in the figure, a null-string translation pattern is created and put into partition PLAR1234. The transformation mask is 1234. The translation pattern has a CSS assigned which includes partition Phones.

Phone1, the phone for which PLAR should be enabled, is configured with a CSS that contains the PLAR1234 partition.

Two phones exist with directory number 1234: Phone2 is in partition Phones and Phone3 is in partition Hidden.

When Phone1 goes off-hook, the null-string pattern is matched because the phone sends a null-string dialed number to Cisco Unified Communications Manager to indicate that it is off-hook and the partition of the translation pattern is included in the phone CSS. The translation pattern now transforms the dialed null string to 1234 and sends a call routing request to Cisco Unified Communications Manager. This request uses the CSS of the translation pattern (Phones) and therefore only finds a single match (Phone2). The call is extended to Phone2.

Note Phone 3 is only shown to illustrate that the call to the translated number uses the CSS of the translation pattern and therefore does not have access to directory number 1234 in partition Hidden.

If the translation pattern had no CSS configured, the call would fail. The translation pattern cannot find extension 1234 because it only has access to the null partition, but both phones configured with directory number 1234 have partitions assigned.

If Phone1 included additional partitions in its CSS, it would still not be able to dial other directory numbers and PLAR would still be active. This is because translation patterns always have urgent priority enabled and therefore the null string pattern is always the best match (before any additional digits are analyzed). Therefore, a null-string translation pattern that is in the null partition would match all calls placed from all phones. In order to avoid breaking telephony services by accidentally enabling such a pattern, Cisco Unified Communications Manager does not allow null-string translation patterns to be added if no partition is assigned.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Calling privileges are implemented to implement class of service or special applications that require calls to be treated differently depending on the caller.
- Partitions are groups of called numbers with identical reachability characteristics. CSS are lists of partitions, that the owner of the CSS has access to.
- Time Schedules and Time Periods are used to activate or deactivate partitions within a CSS depending on time and or date information.
- Client Matter Codes are used to track calls to certain clients by requesting the CMC to be entered and adding it into CDR. FAC are used to allow access to route patterns only if an authorization code with a high-enough level is entered when requested.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-59

Summary (Cont.)

- Calling privileges applications include implementation of class of service, vanity numbers, time-based route or carrier selection, and PLAR.
- Complexity of CoS implementation at IP phones can be reduced by using the line device approach, which allows the effective CSS to be composed of a line and device CSS (in this order).
- Vanity numbers provide access to local services by dialing the same number from any physical location.
- Time schedules and time periods can be used to route calls via different gateways or carriers, depending on the time of the day or date in order to take advantage of the cheapest rate at any time.
- PLAR, a function in which a phone is automatically connected to a predefined number when it goes off-hook, is implemented by using null string translation patterns, partitions, and CSS.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-60

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager Administration Guide Release 6.0(1)
[http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfg/bccm.pdf](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf)
- Cisco Unified Communications Manager System Guide Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmsys/accm.pdf
- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html

Lesson 5

Implementing Call Coverage in Cisco Unified Communications Manager

Overview

Many businesses have sales or service support departments that work as groups to handle inbound calls from customers. These businesses typically need several phone lines and a method to make the lines work together so that if one representative is busy or not available, the call will rotate to other members of the group until it is answered or forwarded to an auto-attendant or voice mail. Hunt groups are the mechanisms that help these businesses manage inbound calls. A hunt group is a group of telephone lines that are associated with a common number. When a call comes in to the number associated with the hunt group, the call cycles through the group of lines until an available line is found. This process is known as hunting.

This lesson describes how to implement hunt groups and enable other call coverage features such as call forwarding, shared lines, and Call Pickup.

Objectives

Upon completing this lesson, you will be able to describe and configure call coverage components in Cisco Unified Communications Manager. This ability includes being able to meet these objectives:

- List call coverage options in Cisco Unified Communications Manager
- Describe call forwarding, shared lines, and Call Pickup
- Describe call hunting implementation in Cisco Unified Communications Manager
- Describe call hunting options and line group distribution algorithms

Cisco Unified Communications Manager Call Coverage Features

This topic describes call coverage features in Cisco Unified Communications Manager.

Call Coverage Features

Call coverage ensures that all incoming calls are answered:

- Used for individuals:
 - Ring other phones if original called phone is not answering (Call forwarding feature)
 - Ring multiple phones at the same time (Shared number)
 - Pick up a call ringing on other phone (Call Pickup/Group Pickup)
- Used for user groups with pilot numbers:
 - Hunt through multiple phones (Call hunting feature)
 - Ring multiple phones (Call hunting with broadcast option)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-4

Call coverage is part of the dial plan. It ensures that all incoming calls are answered. The following call coverage features are typically implemented for individuals:

- **Call forwarding:** If the called phone does not answer the call, the call should be forwarded to another phone or voice mail.
- **Shared lines:** A shared line is a directory number that is assigned to more than one device, allowing the call to be accepted on more than one phone.
- **Call Pickup:** Call Pickup allows a call that is ringing on a phone to be picked up at another phone.

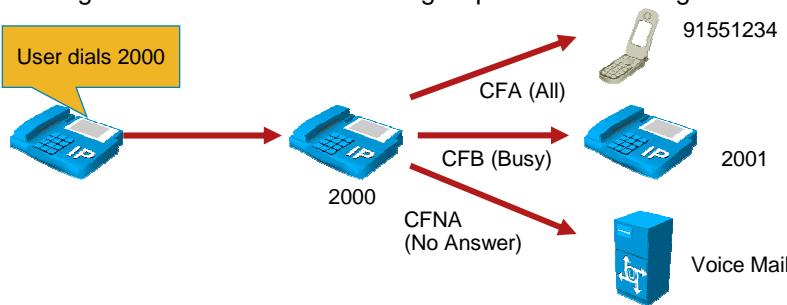
In addition, call hunting is another complex and flexible feature providing call coverage. Call hunting is based on a pilot number that, if directly called or used as a call forward target, allows hunting through multiple line groups. Several hunting algorithms exist, ranging from a round-robin selection of group members to a broadcast option that rings all members of a line group.

Cisco Unified Communications Manager Call Forwarding, Shared Lines, and Call Pickup

This topic describes the call forwarding, shared lines, and Call Pickup features in Cisco Unified Communications Manager.

Call Forwarding

- CFA, CFNA, and CFB are configured under directory number settings.
- CFA is configurable by end user from phone or user web page.
- CFNA and CFB are configurable by end user from user web page.
- If CFA is configured, the call will be forwarded immediately to the configured number. The forwarding IP phone will not ring.



There are three types of call forwarding:

- **Call Forward All (CFA):** CFA means that all calls are forwarded unconditionally. CFA can be configured by the phone user either from the user web page or at the phone itself. If CFA is configured, the call is forwarded immediately without ringing the originally dialed phone.

Note More information about the user web page is provided in the last module of this course.

- **Call Forward No Answer (CFNA):** CFNA forwards calls if the call is not answered within a specified amount of time. CFA can be configured by the administrator in Cisco Unified Communications Manager Administration or by the phone user from the user web page.
- **Call Forward Busy (CFB):** CFB forwards calls that are received while the IP phone is in use with another call. CFB can be configured by the administrator in Cisco Unified Communications Manager Administration or by the phone user from the user web page.

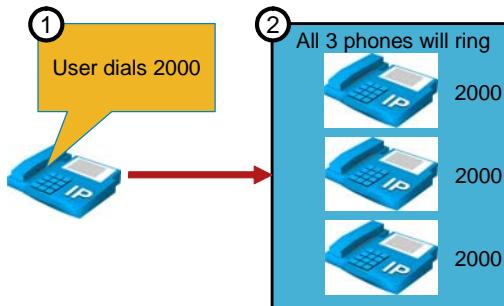
You can configure separate calling search spaces (CSSs) for each call forward type. For CFNA and CFB, different CSSs can be set for internal calls and for external calls. For CFA, a primary and a secondary CFA can be configured, which can be concatenated similarly to a device and line CSS. For all call forward scenarios, the corresponding call forward CSSs are used; line and device CSSs are ignored. Therefore, if the system uses partitions, it is recommended to always set call forward CSSs, because otherwise forward operations are likely to fail.

Shared Lines

This subtopic describes the shared line feature in Cisco Unified Communications Manager.

Shared Lines

- Same directory number configured on multiple phones.
- All phones will ring at the same time if directory number is called.
- A user will pick up the call from one of the phones. All phones stop ringing when the call is answered.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-7

A shared line is implemented by assigning the same directory number to multiple phones. If the number is called, all phones that are configured with this share line number will ring. The first user that accepts the call is connected to the caller and all other phones stop ringing.

Call Pickup/Group Call Pickup

This section describes the Call Pickup feature in Cisco Unified Communications Manager.

Call Pickup/Group Call Pickup

Multiple lines can be grouped together into a pickup group

- Each pickup group is identified by a unique pickup group number.
- Each phone line can be a member of one pickup group.

Call Pickup

- Allows a user to answer a call that is ringing on a phone in the same pickup group as the phone of the user.

Group Call Pickup

- Allows a user to answer a call ringing on any phone that is in a different pickup group than the phone of the user.
- Requires the user to enter the pickup group number.

© 2008 Cisco Systems, Inc. All rights reserved.

CPT1 v6.0—4-8

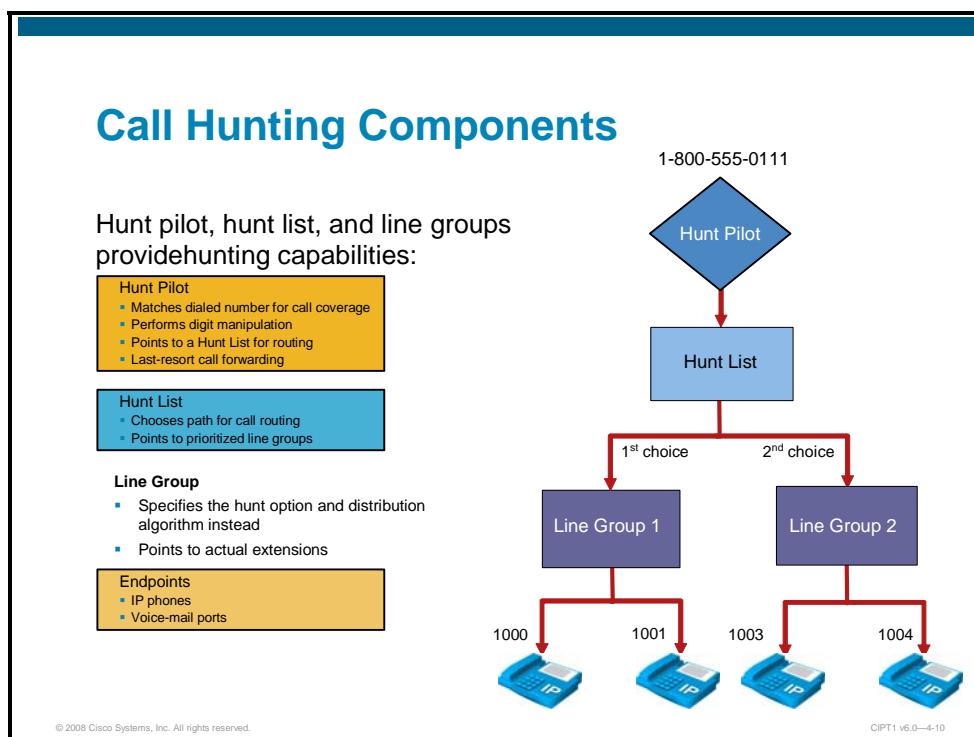
Cisco Unified Communications Manager allows multiple lines to be grouped into pickup groups. Each pickup group is identified by a unique pickup group number, which is part of the call routing table of Cisco Unified Communications Manager. A phone line can be assigned to one pickup group.

If a phone rings but there is nobody to answer the call, another user can pick up the call by using the Call Pickup feature if the ringing phone is in the same pickup group as the phone of the user who wants to pick up the call.

In the same situation, if the phone of the user who wants to pick up the call is *not* a member of the pickup group of the ringing phone, the user can use the Group Call Pickup feature to pick up the call. When a user invokes the Group Call Pickup feature by pressing the corresponding softkey, the user has to enter the pickup group number of the ringing phone to be able to pick up the call.

Call Hunting Components

This topic describes the call hunting feature in Cisco Unified Communications Manager.



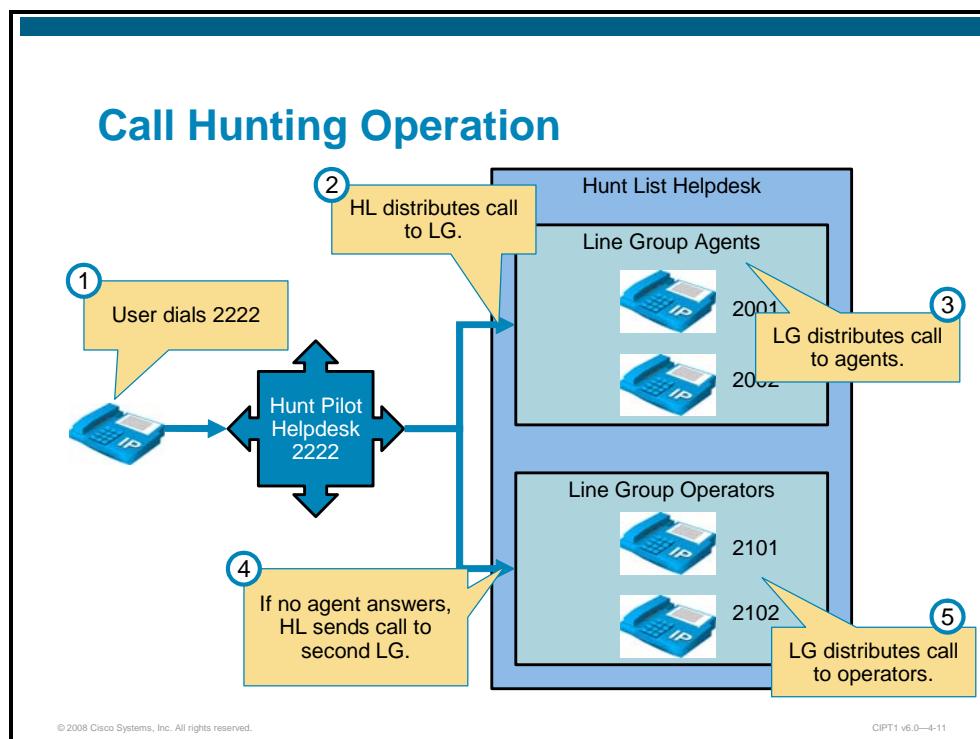
Cisco Unified Communications Manager call hunting implementation is comprised of the following components:

- **Phone directory numbers or voice-mail ports:** Assigned to line groups
- **Line groups:** Assigned to hunt lists. A hunt list can have one or more line groups. At the line group, hunt options and distribution algorithms can be specified in order to define how call hunting should be performed for the members of a line group.
- **Hunt lists:** Assigned to hunt pilots. A hunt list is an ordered list of line groups.
- **Hunt pilots:** The numbers that have been dialed to invoke a hunting process. A hunt pilot can be called directly (for example, to provide a certain service to customers) or a call can be forwarded to the hunt pilot from an IP phone that received a call and is configured to forward calls to the hunt pilot to provide call coverage.

While hunting, the forwarding configuration of line group members is not used. If the hunting algorithm rings a phone and the call is not answered, the CFNA setting of that phone is ignored and the hunting algorithm goes on to the next line group member.

Call Hunting Operation

This subtopic describes call hunting operation.



In the example in the figure, two line groups are configured: Agents (containing directory numbers 2001 and 2002) and Operators (containing directory numbers 2101 and 2102).

The line groups are assigned to the hunt list Helpdesk.

A hunt pilot, Helpdesk, with the pattern 2222, is configured to use hunt list Helpdesk for call coverage.

The following high-level steps describe how this hunt pilot will process calls:

- Step 1** A user dials 2222, matching the hunt pilot number. The hunt pilot sends the call to the hunt list Helpdesk.
- Step 2** The hunt list picks the first line group, Agents.
- Step 3** The line group distributes the call to the assigned agent directory numbers.
- Step 4** If no agent answers, the hunt list sends the call to the second line group, Operators.
- Step 5** The line group Operators distributes the call to the operator directory numbers.

Hunt Pilots

This subtopic describes hunt pilots.

Hunt Pilots

Hunt pilots are configured with a hunt pilot number – the number that needs to be called to start a hunting process.

- Perform digit manipulation
- Point directly to a hunt list
- Specify the maximum hunt timer
- Specify final forwarding settings (on hunt exhaustion)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-12

Hunt pilots are dialable patterns in the call routing table, similar to route patterns and directory numbers. The hunt pilot points directly to a hunt list. Hunt lists point to line groups, which finally point to endpoints.

At the hunt list, digit manipulation can be configured in order to transform the calling and called number before the call is passed on to line group members.

Beginning with Cisco Unified CallManager Release 4.1, calls can be redirected to a final destination when the hunting fails because of one or both of the following reasons:

- All hunting options have been exhausted and the call still is not answered.
- A maximum hunt timer, configured at the hunt list, has expired.

This call redirection is configured in the Hunt Forward Settings section of the hunt pilot configuration page, and the destination for this redirect can be either of the following options:

- A specific destination configured globally at the hunt pilot.
- A personal preference, configured at the phone line of the originally called number when hunting on behalf of that number fails. The personal preference is configured using the Call Forward No Coverage (CFNC) settings at the phone line.

For example, you can implement the personal preferences option by configuring a user phone so that the Forward No Answer field redirects the call to a hunt pilot, in order to search for someone else who can answer the call. If the call hunting fails, either because all the hunting options were exhausted or because a timeout period expired, the call can be sent to a destination personalized for the person who was originally called. For example, if you set the Forward No Coverage field in the directory number configuration page to a voice-mail number, the call will be sent to the voice-mail box of that person if hunting fails.

The following considerations apply to calls handled by hunt pilots:

- Call Pickup and Group Call Pickup are not supported on calls distributed by a hunt pilot. A member of the line group cannot pick up the hunt pilot call offered to another member in the line group, even if they belong to the same call pickup group.
- The hunt pilot can distribute calls to any of its line group members, regardless of calling privilege implementation at the line group member. If line group members are configured with a partition, the hunt pilot overcomes all partitions and CSS restrictions.

Hunt Lists

This subtopic describes hunt lists.

Hunt Lists

A hunt list is a prioritized list of line groups.

- Multiple hunt pilots may point to the same hunt list.
- Multiple hunt lists can contain the same line group.
- Hunt lists do not perform digit manipulation.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-13

A hunt list is a prioritized list of line groups used for call coverage. Hunt lists have the following characteristics:

- Multiple hunt pilots can point to the same hunt list.
- Multiple hunt lists can contain the same line group.
- A hunt list is a prioritized list of line groups; line groups are hunted in the order of their configuration in the hunt list.
- A hunt list does not perform digit manipulation.

Line Groups

This subtopic describes line groups.

Line Groups

Line groups control the order in which a call is distributed among the line group members.

- Line groups point to specific extensions, typically IP phone extensions or voice-mail ports.
- The same extension may be contained in multiple line groups
- The hunt option describes how to continue hunting after trying the first member of the line group (stop hunting, switch immediately to next line group, try remaining line group members, then go to next line group).
- The distribution algorithm specifies the order in which the line group members are hunted (circular, longest idle, broadcast, or member that follows the last used).
- The Ring No Answer Reversion (RNAR) timeout value specifies how long to try a member of the line group.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-14

Line groups control the order in which a call is distributed, and they have the following characteristics:

- Line groups point to specific extensions, which are typically IP phone extensions or voice-mail ports.
- The same extension may be present in multiple line groups.
- Line groups are configured with a global distribution algorithm which is used to select the next line group member for hunting.
- Line groups are configured with a hunt option which describes how hunting should be continued after trying the first member of the line group. The hunt option is configured per hunt failure event: no answer, busy, and not available.
- The Ring No Answer Reversion (RNAR) timeout specifies how long the hunting algorithm rings a member of the line group before it proceeds to hunt according to the line group no answer hunt option setting.

Line Group Members

This subtopic describes line group members.

Line Group Members

Line group members are the endpoints accessed by line groups, and they can be any of the following types:

- Any SCCP endpoints, such as Cisco Unified IP phones, VG248, or ATA 188
- SIP endpoints
- Voice-mail ports
- H.323 clients
- FXS extensions attached to an MGCP gateway

Note: CTI ports and CTI route points cannot be added within a line group. Calls cannot be distributed to endpoints controlled through CTI applications (CRS, IP IVR, etc.)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-15

Line group members are the endpoints accessed by line groups, which can be any of the following types:

- Any Skinny Client Control Protocol (SCCP) endpoints, such as Cisco Unified IP phones, Cisco VG248 Analog Phone Gateway, or Cisco ATA 188
- Session initiation protocol (SIP) endpoints
- Voice-mail ports
- H.323 clients
- Foreign Exchange Station (FXS) extensions attached to a Media Gateway Control Protocol (MGCP) gateway

Computer telephony integration (CTI) ports and CTI route points cannot be added to a line group. Therefore, calls cannot be distributed to endpoints controlled through CTI applications such as Cisco Customer Response Solution (CRS), Cisco Unified IP Interactive Voice Response (IVR), and so on.

Call Hunt Options and Distribution Algorithms

This topic describes the available call hunt options and distribution algorithms.

Line Group Hunt Options

After trying a member of a line group, the hunt option specifies how to continue hunting, depending on the result of the last attempt (no answer, busy, and not available):

- Try Next Member, Then, Try Next Group in Hunt List (Default):
 - Sends the call to idle or available members. If no more members, try the next line group of the hunt list. If no more line groups, hunting stops.
- Try Next Member, but Do Not Go to Next Group:
 - Sends the call to idle or available members. If no more members, hunting stops.
- Skip Remaining Members, and Go Directly to Next Group:
 - Sends the call to the next line group. If no more line groups, hunting stops.
- Stop Hunting:
 - Hunting stops.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-17

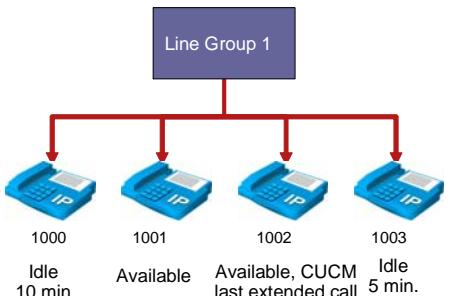
After trying a line group member, in the event of no answer, busy, or not available, the way that hunting continues depends on the line group hunt option, which is configured per event (no answer, busy, and not available), as follows:

- **Try Next Member, Then, Try Next Group in Hunt List (Default):** Send the call to the next idle or available member of this line group. If no more members are available in this line group, go to the next line group configured in the hunt list. If no more line groups are available, hunting stops.
- **Try Next Member, but Do Not Go to Next Group:** Send the call to the next idle or available member of this line group. If no more members are available in this line group, hunting stops.
- **Skip Remaining Members, and Go Directly to Next Group:** Send the call to the next line group. If no more line groups are available, hunting stops.
- **Stop Hunting**

Line Group Distribution Algorithms

This subtopic describes the available distribution algorithms in Cisco Unified Communications Manager call hunting.

Line Group Distribution Algorithms



The diagram illustrates a line group distribution algorithm. At the top is a blue box labeled "Line Group 1". Four red arrows point from this box to four blue telephone icons below it, each labeled with a directory number: 1000, 1001, 1002, and 1003. Below each telephone icon is its status and idle time:
1000: Idle, 10 min.
1001: Available
1002: Available, CUCM last extended call
1003: Idle, 5 min.

The line group distribution algorithm specifies the order in which line group members are hunted.

- Top down: Idle and available members, round-robin. (Next call to 1000.)
- Circular: $(n + 1)$ th member where n is the member to which Unified CM most recently extended call. (Next call to 1003.)
- Longest idle time: Idle members only, from most to least idle. (Next call to 1000.)
- Broadcast: All idle and available members simultaneously. (Next call to all directory numbers.)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-18

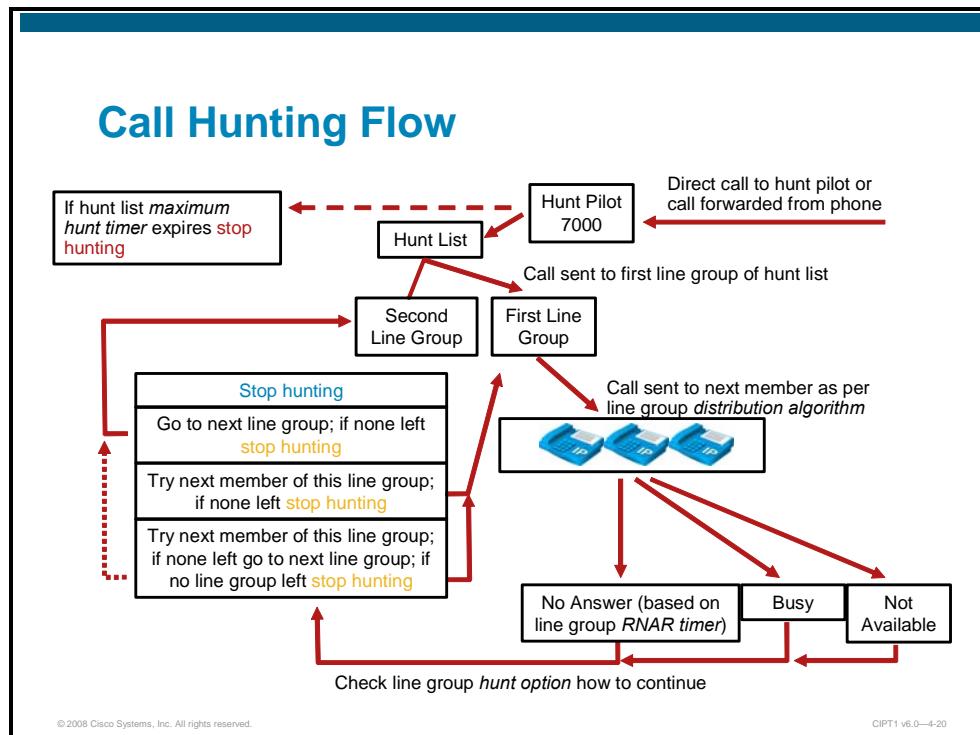
The line group distribution algorithm specifies the order in which line group members should be used during the hunting process. The available algorithms are as follows:

- **Top down:** If you choose a top-down distribution algorithm, Cisco Unified Communications Manager distributes the call to idle or available members, starting from the first idle or available member of a line group to the last idle or available member. This method is also called round-robin distribution. In the figure, a top-down distribution algorithm would extend the next call to 1000, then to 1001, then to 1002, then to 1003, and back to 1000.
- **Circular:** If you choose a circular distribution algorithm, Cisco Unified Communications Manager distributes the call to idle or available members starting from the $(n+1)$ th member of a line group, where the n th member is the member to which Cisco Unified Communications Manager most recently extended a call. If the n th member is the last member of a line group, Cisco Unified Communications Manager distributes the call to the first idle or available member of the line group. In the figure, assume that Cisco Unified Communications Manager extended the last call to 1002 (n). The next call that comes in on the hunt pilot number would go to 1003 ($n + 1$).
- **Longest idle time:** If you choose a longest-idle-time distribution algorithm, Cisco Unified Communications Manager distributes the call to the idle member which has been idle for the longest time. Available members are not considered by this distribution algorithm. In the figure, assume that 1000 has been idle for 10 minutes and 1003 has been idle for 5 minutes. A longest-idle-time distribution mechanism would extend the call to 1000.
- **Broadcast:** If you choose a broadcast distribution algorithm, Cisco Unified Communications Manager distributes the call to all idle or available members of a line group simultaneously.

Distribution algorithms are configured once per line group in Cisco Unified Communications Manager Administration.

Call Hunting Flow

This topic describes the call hunting flow in a Cisco Unified Communications Manager call hunting configuration.

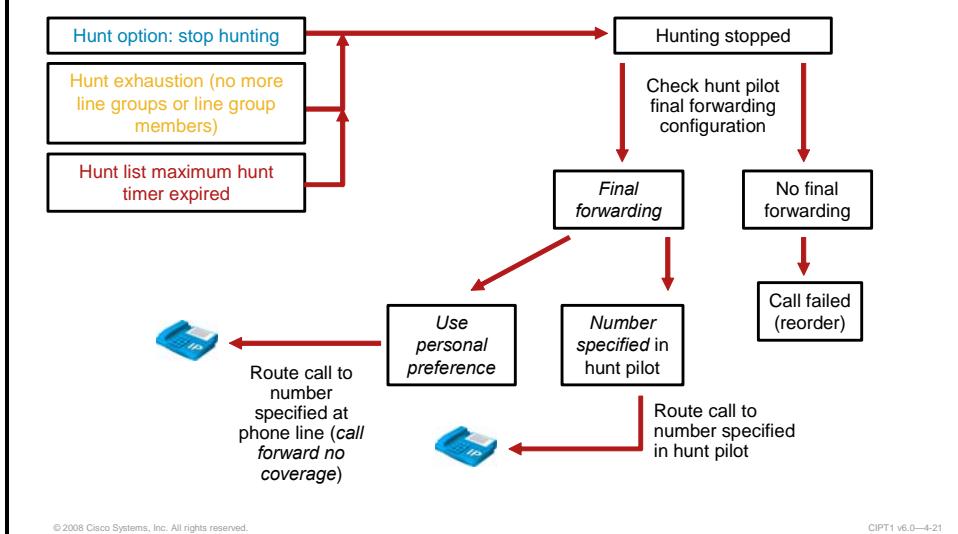


The call hunting flow in Cisco Unified Communications Manager call hunting configuration is as follows:

- Step 1** A direct call is placed to the hunt pilot number or a call is forwarded to the hunt pilot number from a phone.
- Step 2** The hunt pilot configured with the appropriate hunt pilot number starts the maximum hunt timer to monitor the overall hunting time. If the timer expires, hunting stops. The hunt pilot is associated with a hunt list.
- Step 3** The hunt list that is associated with the hunt pilot sends the call to the next line group configured in the hunt list (starting with the first).
- Step 4** The line group sends the call to the next line group member based on the distribution algorithm configured at the line group. The possible distribution methods are:
 - Top down
 - Circular
 - Longest idle time
 - Broadcast
- Step 5** If the line group member (or members in case of broadcast) selected by the distribution algorithm do not answer the call, the hunt option which is configured independently per hunt failure reason at the line group specifies how hunting should be continued. Possible hunt failure reasons are: no answer (i.e. the expiration of the RNAR timer, configured at the line group), busy, and not available.

- If the hunt option configured for the appropriate hunt failure reason is Stop Hunting, hunting stops.
- If the hunt option configured for the appropriate hunt failure reason is Skip Remaining Members, and Go Directly to Next Group, and there are no more line groups, hunting stops. If there are additional line groups, go to Step 4 to see how the process continues with the next line group.
- If the hunt option configured for the appropriate hunt failure reason is Try Next Member, but Do Not Go to Next Group, and there are no more line group members, hunting stops. If there are additional line group members, go to Step 4 to see how the process continues with the next line group member.
- If the hunt option configured for the appropriate hunt failure reason is Try Next Member, Then, Try Next Group in Hunt List, and there are additional line group members, go to Step 4 to see how the process continues with the next line group member. If there are no additional line group members, the next line group is to be used. If there are additional line groups, go to Step 4 to see how the process continues with the next line group. If there are no more line groups, hunting stops.

Call Hunting Flow (Cont.)



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-21

When hunting stops, the following are possible reasons:

- The hunt option that had to be applied after a call was not accepted by the last line group member tried was Stop Hunting.
- Hunt exhaustion: After the last line group member tried, there were no other line group members and no other line groups left to be used.
- Expiration of the maximum hunt timer configured at the hunt pilot.

The process continues as described in the following steps:

Step 1 Check the hunt pilot configuration for its final forwarding settings.

- If the hunt pilot is not configured for final forwarding, the call fails and a reorder tone is played.

Step 2 Check the final forwarding destination settings configured at the hunt pilot.

- If a final forwarding number is specified at the hunt pilot, route the call to the specified number.
- If Use Personal Preference is selected, route the call to the number that is configured for Call Forward No Coverage at the phone line that invoked the call to the pilot number.

Call Hunting Configuration

This topic describes how to configure call hunting in Cisco Unified Communications Manager.

Configuring Line Groups, Hunt Lists, and Hunt Pilots

1. Create line group, add directory numbers, and determine distribution algorithm and hunt options
2. Create hunt list and add line groups
3. Create hunt pilot, associate hunt list, and configure hunt forward settings
4. Configure personal preference on phones in case of no hunt coverage

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-23

To access the line group, hunt list, and hunt pilot configuration windows in Cisco Unified Communications Manager Administration, choose **Call Routing > Route/Hunt**.

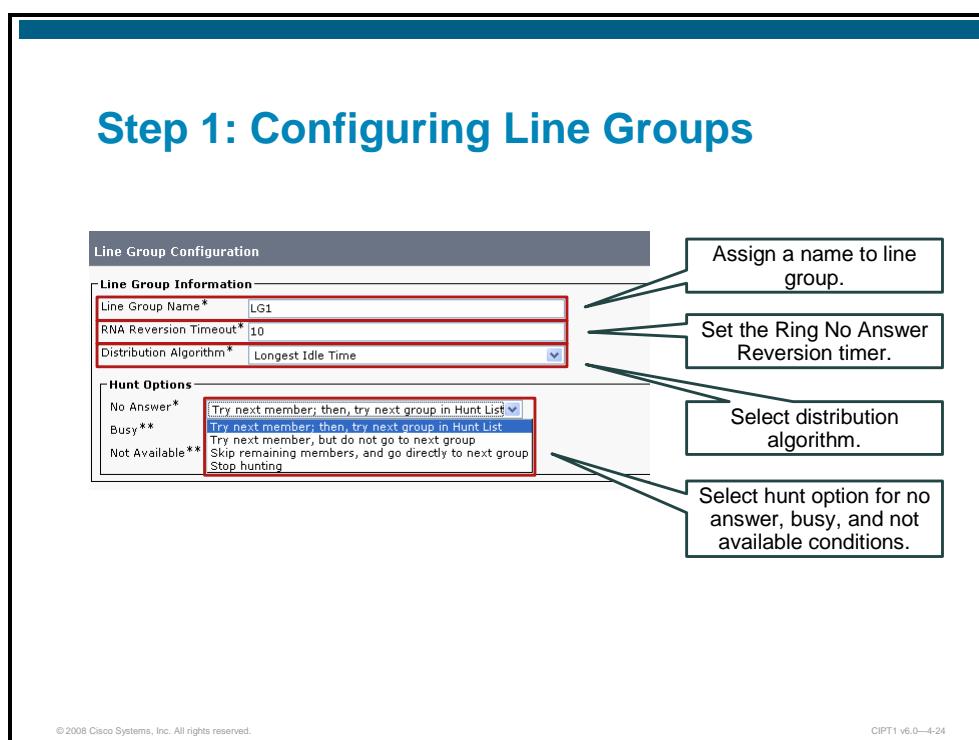
When configuring hunting, follow these steps:

- Step 1** Create the line groups, add members, and configure the distribution algorithm and hunt options.
- Step 2** Create the hunt list and add the line groups.
- Step 3** Create the hunt pilot, associate the hunt list with the hunt pilot, and configure hunt forward settings.
- Step 4** Configure personal preferences on phone lines in the event that hunting ends with no coverage.

Note	Use concise and descriptive names for your line groups and hunt lists. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a line group. For example, CiscoDallasAA1 may identify a Cisco Access Analog line group for the Cisco office in Dallas.
-------------	---

Step 1: Configuring Line Groups

The figure shows how to configure line groups.

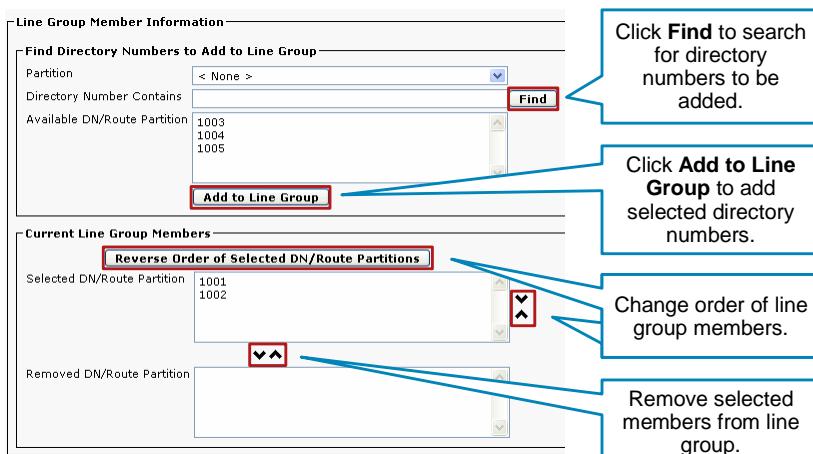


The directory numbers that will become the members of the line group must already exist in the database before you can complete this procedure. Follow these steps to configure line groups:

- Step 1** Choose **Call Routing > Route/Hunt > Line Group** from the menu.
- Step 2** Click **Add New**.
- Step 3** Enter a name in the Line Group Name field. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each line group name is unique to the route plan.
- Step 4** Configure the distribution algorithm, hunt options, and RNAR timeout as desired, or leave them at their default values.

Note	Options for the distribution algorithm are: Top Down, Circular, Longest Idle Time, and Broadcast. Hunt options are Try Next Member, Then, Try Next Group in Hunt List, Try Next Member, but Do Not Go To Next Group, Skip Remaining Members, and Go Directly to Next Group, and Stop Hunting. The RNAR timer specifies how long to try one member before ending in a no answer condition. The default value is 10 seconds.
-------------	--

Step 1: Configuring Line Groups (Cont.)



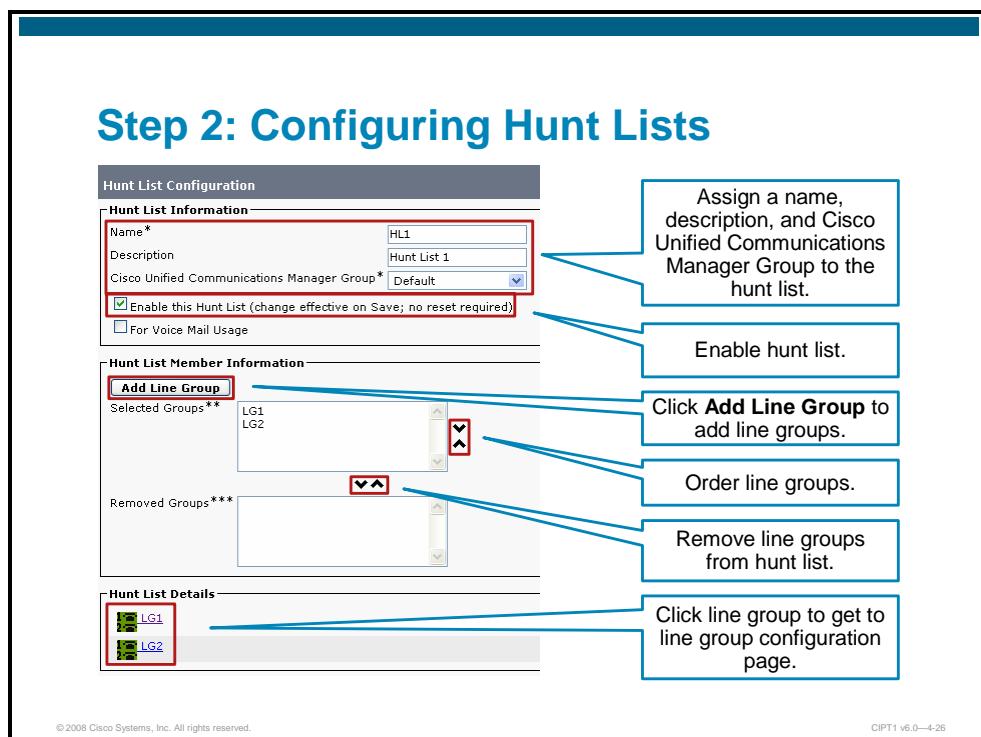
© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-25

- Step 5** Add members to the line group. If you need to locate a directory number, choose a route partition from the Partition drop-down list, enter a search string in the Directory Number Contains field, and click **Find**. To find all directory numbers that belong to a partition, leave the Directory Number Contains field blank and click **Find**. A list of matching directory numbers is displayed in the Available DN/Route Partition pane.
- Step 6** In the Available DN/Route Partition pane, select a directory number to add and click **Add to Line Group** to move it to the Selected DN/Route Partition pane. Repeat this step for each member that you want to add to this line group.
- Step 7** In the Selected DN/Route Partition pane, choose the order in which the new directory numbers will be accessed in this line group. To change the order, click a directory number and use the Up and Down arrows to the right of the pane.
- Step 8** Click **Save** to add the new directory numbers and to update the directory number order for this line group.

Step 2: Configuring Hunt Lists

The figure shows how to configure hunt lists.



To add a hunt list, follow these steps:

- Step 1** Choose **Call Routing > Route/Hunt > Hunt List**.
- Step 2** Click **Add New**.
- Step 3** In the Name field, enter a name. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each hunt list name is unique to the route plan. Enter a descriptive name in the Description field.
- Step 4** Choose a Cisco Unified Communications Manager group from the drop-down list. The group must already exist in the database; you cannot create a new group from this window.
- Step 5** To add this hunt list, click **Save**. The Hunt List Configuration window displays the newly added hunt list.
- Step 6** Add at least one line group to the new hunt list. To add a line group, click **Add Line Group**. The Hunt List Detail Configuration window is displayed.
- Step 7** From the Line Group drop-down list, choose a line group to add to the hunt list. To add the line group, click **Save**. The popup window appears, stating that, for the changes to take effect, you must reset the hunt list. Click **OK** to confirm the message. The line group name is displayed in the Selected Group list on the right side of the window.
- Step 8** To add more line groups to this list, click **Add Line Group** and repeat the previous two steps.

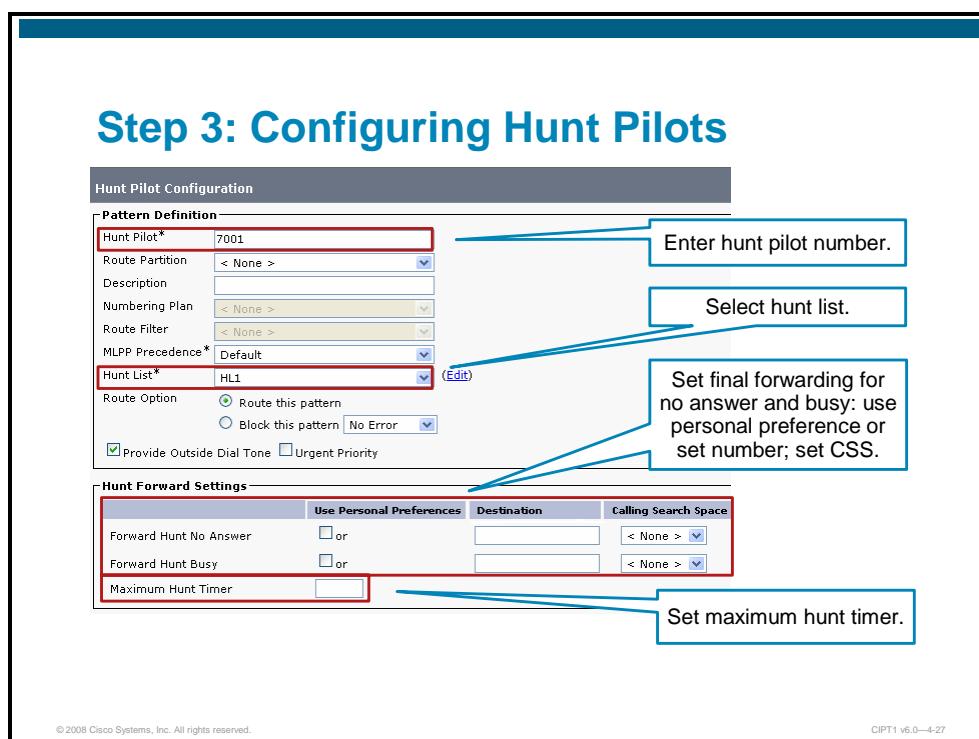
Step 9 When you finish adding line groups to the hunt list, click **Save**.

Step 10 Click **OK** in the popup window to reset the hunt list.

Cisco Unified Communications Manager accesses line groups in the order in which they are shown in the hunt list. The access order of line groups is changed by selecting a line group from the Selected Groups pane and clicking the Up or Down arrow on the right side of the pane to move the line group up or down in the list.

Step 3: Configuring Hunt Pilots

The figure shows how to configure hunt pilots.



Follow these steps to configure a hunt pilot:

- Step 1** Choose **Call Routing > Route/Hunt > Hunt Pilot** from the menu.
- Step 2** Click **Add New**.
- Step 3** Enter the hunt pilot number in the Hunt Pilot field.
- Step 4** Assign the hunt pilot to a hunt list using the Hunt List drop-down menu.
- Step 5** Configure final forwarding settings and set the maximum hunt timer.
- Step 6** When finished, click **Save**.

The Hunt Forward Settings area of the Hunt Pilot Configuration window specifies the final forwarding settings and maximum timer values, as shown in the table.

Hunt Forward Settings

Setting	Description
Forward Hunt No Answer	<p>When the call distributed through the hunt list is not answered within a specific period of time, this field specifies the destination to which to forward the call. Choose from these options:</p> <ul style="list-style-type: none"> ■ Use Personal Preferences: Enables the CFNC settings for the original called number that forwarded the call to this hunt pilot. The CFNC setting specifies a call forwarding reason that you administer in the Directory Number Configuration window. Calls are diverted based on the value in the Coverage/Destination field of the directory number when a call to the directory number first diverts to coverage, and coverage either exhausts or times out, and the associated hunt pilot for coverage specifies Use Personal Preferences for its final forwarding. When the Use Personal Preferences check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination and Calling Search Space fields. ■ Destination: This setting indicates the directory number to which calls are forwarded. ■ Calling Search Space: This setting applies to all devices that are using this directory number.
Forward Hunt Busy	<p>When the call distributed through the hunt list encounters only busy lines for a specific period of time, this field specifies the destination to which to forward the call. Choose from these options:</p> <ul style="list-style-type: none"> ■ Use Personal Preferences: Use this check box to enable the CFNC settings for the original called number that forwarded the call to this hunt pilot. When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination and Calling Search Space fields. ■ Destination: This setting indicates the directory number to which calls are forwarded. ■ Calling Search Space: This setting applies to all devices that are using this directory number.
Maximum Hunt Timer	Specifies the maximum time for hunting (in seconds).

Directory Number Configuration

The figure shows how to configure call forward at IP phones when implementing call coverage.

Step 4: Configure Call Forward No Coverage (CFNC) at Directory Numbers

Call Forward and Call Pickup Settings		Voice Mail	Destination	Calling Search Space
Calling Search Space Activation Policy				
Forward All	<input type="checkbox"/> or	<input type="text" value=""/>	<input type="button" value="..."/>	Use System Default <input type="button" value="..."/> <input type="button" value="..."/>
Secondary Calling Search Space for Forward All				
Forward Busy Internal	<input type="checkbox"/> or	<input type="text" value="7001"/>	<input type="button" value="..."/>	<input type="button" value="..."/> <input type="button" value="..."/>
Forward Busy External	<input type="checkbox"/> or	<input type="text" value="9010"/>	<input type="button" value="..."/>	<input type="button" value="..."/> <input type="button" value="..."/>
Forward No Answer Internal	<input type="checkbox"/> or	<input type="text" value="7002"/>	<input type="button" value="..."/>	<input type="button" value="..."/> <input type="button" value="..."/>
Forward No Answer External	<input type="checkbox"/> or	<input type="text" value="7002"/>	<input type="button" value="..."/>	<input type="button" value="..."/> <input type="button" value="..."/>
Forward No Coverage Internal	<input type="checkbox"/> or	<input type="text" value=""/>	<input type="button" value="..."/>	<input type="button" value="..."/> <input type="button" value="..."/>
Forward No Coverage External	<input type="checkbox"/> or	<input type="text" value="93035555000"/>	<input type="button" value="..."/>	<input type="button" value="..."/> <input type="button" value="..."/>
Forward on CTI Failure	<input type="checkbox"/> or	<input type="text" value=""/>	<input type="button" value="..."/>	<input type="button" value="..."/> <input type="button" value="..."/>
Forward Unregistered Internal	<input type="checkbox"/> or	<input type="text" value="7002"/>	<input type="button" value="..."/>	<input type="button" value="..."/> <input type="button" value="..."/>
Forward Unregistered External	<input type="checkbox"/> or	<input type="text" value="7002"/>	<input type="button" value="..."/>	<input type="button" value="..."/> <input type="button" value="..."/>
No Answer Ring Duration (seconds)				
Call Pickup Group <input type="button" value="..."/>				

Settings to support final forwarding per personal preference (internal and external).

Separate configuration capability for internal CFNA and external CFNA.

Separate configuration capability for internal CFB and external CFB.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-28

The Directory Number Configuration window provides configuration options for internal and external forwarding based on whether a call is CFA or CFNA, as specified in the table.

Call Forward and Pickup Settings

Field	Description
Forward All	<p>Specifies the forwarding treatment for calls to this directory number if the directory number is set to forward all calls.</p> <ul style="list-style-type: none">■ Voice Mail: Check this check box to use settings in the Voice Mail Profile Configuration window. When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination and Calling Search Space fields.■ Destination: This setting indicates the directory number to which all calls are forwarded. Use any dialable phone number, including an outside destination.■ Calling Search Space: This setting applies to all devices that are using this directory number.
Forward Busy Internal Forward Busy External	<p>Specifies the forwarding treatment for internal or external calls to this directory number if the directory number is busy.</p> <ul style="list-style-type: none">■ Voice Mail: Check this check box to use settings in the Voice Mail Profile Configuration window for internal calls. When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination and Calling Search Space fields.■ Destination: Use any dialable phone number, including an outside destination.■ Calling Search Space: This setting applies to all devices that are using this directory number.

Field	Description
Forward No Answer Internal Forward No Answer External	<p>Specifies the forwarding treatment for internal or external calls to this directory number if the directory number does not answer.</p> <ul style="list-style-type: none"> ■ Voice Mail: Check this check box to use settings in the Voice Mail Profile Configuration window. When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination and Calling Search Space fields. ■ Destination: This setting indicates the directory number to which an internal call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination. ■ Calling Search Space: This setting applies to all devices that are using this directory number.
Forward No Coverage Internal Forward No Coverage External	<p>This setting applies only if you configure one of the other forwarding fields—CFA, CFB, or CFNA—with a hunt pilot number in the Destination directory number field.</p> <p>For the hunt pilot settings, you must also configure the Forward Hunt No Answer or Forward Hunt Busy fields and check the Use Personal Preferences check box under the Hunt Forward Settings section in the Hunt Pilot Configuration window; otherwise, the Forward No Coverage configuration in the Directory Number Configuration window has no effect.</p>

Example 1: Internal and External Forwarding (No Hunting)

The figure shows an example with internal and external forwarding options with no hunting enabled.

Example 1: Internal and External Forwarding (No Hunting)

User A (directory number 3000) wants:

- CFB: Incoming **internal** and incoming **external** calls to forward to 3001 when busy.
- CFNA: Incoming **internal** calls to forward to 3001 and incoming **external** calls to forward to (303) 555-0111 when no answer.

Solution:

Configuration window for 3000 DN

Call Forward and Call Pickup Settings

	Voice Mail Destination
Forward All	<input type="checkbox"/> or <input type="text"/>
Secondary Calling Search Space for Forward All	
Forward Busy Internal	<input type="checkbox"/> or <input type="text" value="3001"/>
Forward Busy External	<input type="checkbox"/> or <input type="text" value="3001"/>
Forward No Answer Internal	<input type="checkbox"/> or <input type="text" value="3001"/>
Forward No Answer External	<input type="checkbox"/> or <input type="text" value="3035550111"/>
Forward No Coverage Internal	<input type="checkbox"/> or <input type="text"/>
Forward No Coverage External	<input type="checkbox"/> or <input type="text"/>
Forward on CTI Failure	<input type="checkbox"/> or <input type="text"/>

© 2008 Cisco Systems, Inc. All rights reserved.

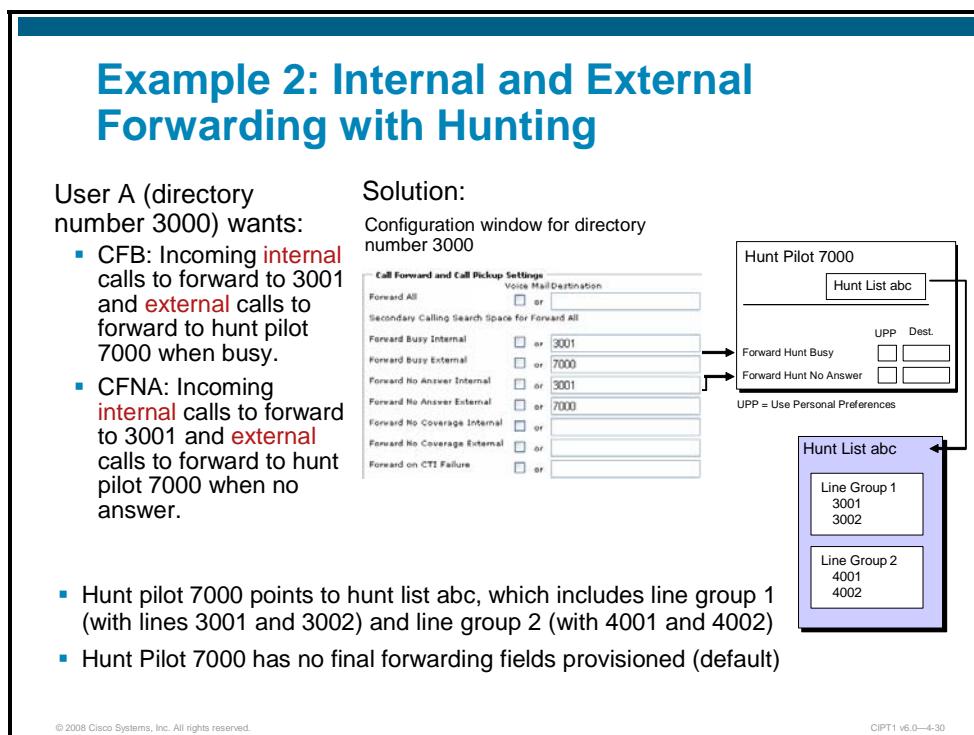
CIPT1 v6.0—4-29

The first example is straightforward. User A at directory number 3000 has the configuration shown in the figure in the Directory Number Configuration window:

- **CFB:** CFB is determined by the Forward Busy Internal and Forward Busy External settings, both set to 3001. This setting forwards incoming internal and incoming external calls to 3001 when 3000 is busy.
- **CFNA:** CFNA is determined by the Forward No Answer Internal and Forward No Answer External settings. This setting forwards incoming internal calls to 3001, and external incoming calls to (303) 555-0111 when 3000 does not answer.

Example 2: Internal and External Forwarding with Hunting

The figure shows an example with internal and external forwarding options with hunting enabled.



User A at directory number 3000 has the configuration shown in the figure in the Directory Number Configuration window:

- CFB:** Incoming internal calls to forward to 3001 and external calls to forward to hunt pilot 7000 when busy.
- CFNA:** Incoming internal calls to forward to 3001, and external forward calls to forward to hunt pilot 7000 when there is no answer.

Assume that hunt pilot 7000 is associated with hunt list abc and has four hunt parties distributed over Line Group 1 and Line Group 2. Hunt pilot 7000 has no final forwarding fields provisioned (default).

Question: What behavior results when an internal caller calls 3000 and user 3000 is busy?

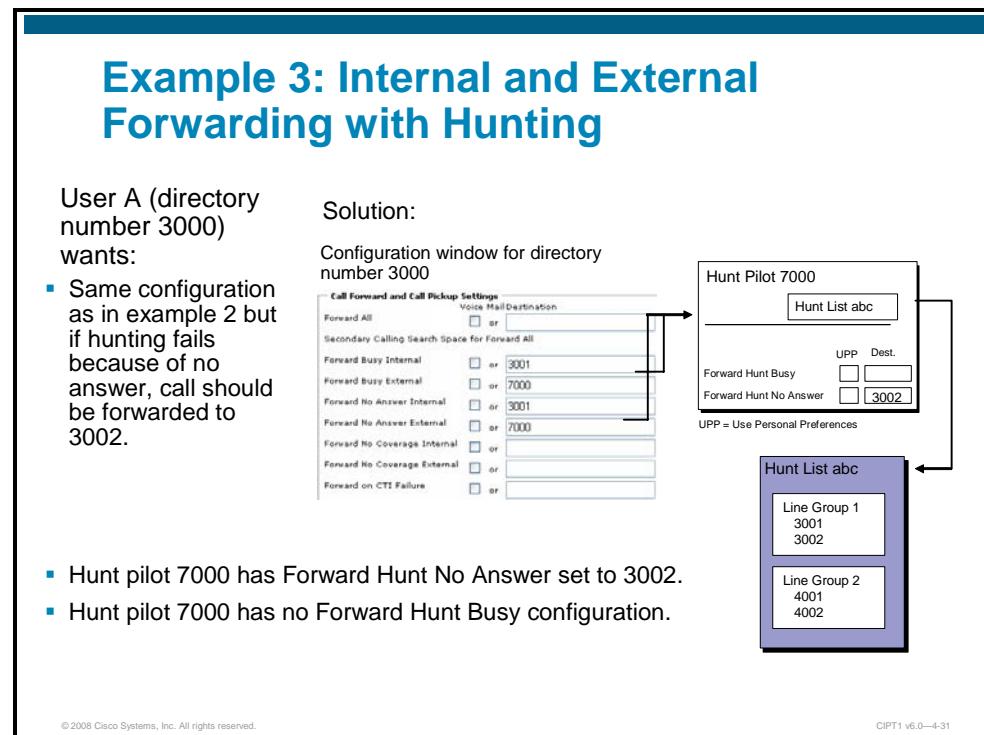
Answer: The call forwards to line 3001.

Question: What behavior results when an external caller calls 3000 and user 3000 does not answer?

Answer: The call forwards to hunt pilot 7000, which will cause hunting to lines 3001, 3002, 4001, and 4002. If one of the hunt parties answers, the caller will be connected to that party. If no hunt party answers, then, regardless of the reason, the caller will receive a reorder tone (or an equivalent announcement).

Example 3: Internal and External Forwarding with Hunting

The figure shows another call hunting example configuration.



Hunt pilot 7000 has Forward Hunt No Answer field set to 3002, but all Forward Hunt Busy fields are empty.

Q: What behavior results when an external caller calls 3000 and user 3000 does not answer?

A: The call will forward to hunt pilot 7000, which will cause hunting to lines 3001, 3002, 4001, and 4002. If one of the hunt parties answers, the caller will be connected to that party.

Otherwise, if all hunt parties are busy, the caller will receive a reorder tone (or an equivalent announcement).

Otherwise, if at least one hunt party is alerted (rings), the call will forward to 3002 because 3002 is the value configured for the Forward Hunt No Answer field.

Q: What if user 3000 is busy when an external call arrives?

A: In this case, the same result occurs because user 3000 forwards external calls to hunt pilot 7000 for both busy and no-answer conditions.

Example 4: Internal and External Forwarding with Hunting

The figure shows an example that extends the previous example by amending some of its forwarding options.

Example 4: Internal and External Forwarding with Hunting

User A (directory number 3000) wants:

- Same configuration as in example 3 but if hunting fails because of busy, call should be forwarded to numbers specified for Forward No Coverage Internal and External at directory number 3000
- Hunt pilot 7000 has Forward Hunt Busy Use Personal Preferences check box activated.
- Forward No Coverage Internal is set to 3005 at line 3000.
- Forward No Coverage External is set to (303) 555-0111 at line 3000.

Solution:

Configuration window for directory number 3000

Call Forward and Call Pickup Settings

Voice Mail Destination: _____

Forward All: or _____

Secondary Calling Search Space for Forward All

Forward Busy Internal: or 3001
 or 7000

Forward Busy External: or 3001
 or 7000

Forward No Answer Internal: or 3001
 or 7000

Forward No Coverage Internal: or 3005

Forward No Coverage External: or (303) 555-0111

Forward on CTT Failure: or _____

Forward Hunt Busy: Dest. _____

Forward Hunt No Answer: Dest. 3002

UPP = Use Personal Preferences

Hunt Pilot 7000

Hunt List abc

Line Group 1
3001
3002

Line Group 2
4001
4002

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-32

Q: What behavior results when an external caller calls 3000 and user 3000 does not answer?

A: The call will forward to hunt pilot 7000, which will cause hunting to lines 3001, 3002, 4001, and 4002.

If one of the hunt parties answers, the caller will be connected to that party. If at least one party is alerted, hunting exhausts because there was no answer, and the call will forward to 3002.

If all hunt parties are busy, the call will forward to the Forward No Coverage External setting of the original called party (user 3000). In this case, the call will forward to the hunt pilot (303) 555-0111.

Q: What if user 3000 is busy when an external call arrives?

A: In this case, the result is the same, because user 3000 forwards external calls to hunt pilot 7000 for both busy or no-answer states.

Note If the hunt pilot is configured to use personal preferences but the corresponding forward no coverage field is not set at the phone, the call will fail. This configuration results in the same behavior as no final forwarding setting at the hunt pilot.

Example 5: Using the Maximum Hunt Timer While Hunting

The figure shows an example in which the maximum hunt timer expires.

Example 5: Using the Maximum Hunt Timer While Hunting

Solution:
Configuration window for directory number 3000

Call Forward and Call Pickup Settings

Forward All	Voice Mail Destination <input type="checkbox"/> or <input type="text"/>
Secondary Calling Search Space for Forward All	
Forward Busy Internal	<input type="checkbox"/> or <input type="text" value="3001"/>
Forward Busy External	<input type="checkbox"/> or <input type="text" value="7000"/>
Forward No Answer Internal	<input type="checkbox"/> or <input type="text" value="3001"/>
Forward No Answer External	<input type="checkbox"/> or <input type="text" value="7000"/>
Forward No Coverage Internal	<input type="checkbox"/> or <input type="text" value="3005"/>
Forward No Coverage External	<input type="checkbox"/> or <input type="text"/>
Forward on CTI Failure	<input type="checkbox"/> or <input type="text"/>

Hunt Pilot 7000

Hunt List abc	UPP Dest. <input checked="" type="checkbox"/> <input type="text"/> Forward Hunt Busy <input type="checkbox"/> <input type="text"/> Forward Hunt No Answer <input type="checkbox"/> <input type="text" value="3002"/>
---------------	---

UPP = Use Personal Preferences

Hunt List abc

Line Group 1 3001 3002	Line Group 2 4001 4002
------------------------------	------------------------------

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-33

The RNAR timer for a line group determines how long hunting will ring a hunt party before moving to the next party in its list (assuming that the customer did not select the broadcast algorithm). This timer has a default value of 10 seconds.

Q: In the examples of four hunt parties, how long will it take before hunting exhausts?

A: It will take 40 seconds before hunting exhausts (10 seconds RNAR x 4 hunt members).

Assume that the maximum hunt timer for hunt pilot 7000 is set to 25 seconds. The call must be answered within this hunt timer. In this example, this hunt timer is 2.5 times the RNAR timer, which is 10 seconds.

Q: What behavior results when a user calls hunt pilot 7000?

A: The call attempts to hunt to the four parties. If no party answers within 25 seconds, hunting terminates and the cause is treated as no answer. Hunting terminates after the third member has been alerted for 5 seconds (10 seconds RNAR on each of the first two members leave 5 seconds before expiration of the 25 seconds maximum hunt time configured at the hunt pilot) and then the call forwards to 3002 because hunting failed with a no answer condition.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Unified CM offers several features for call coverage including call forwarding, shared lines, call pickup, and call hunting.
- In Unified CM, IP phone lines can be configured with call forward all, call forward busy, call forward no answer, call forward no coverage, and call forward unregistered.
- Call hunting in Unified CM uses the following elements: hunt pilots, hunt lists, line groups, and endpoints (lines and voice-mail ports).
- Call hunting options are configured per line group and specify how to continue hunting when the selected line group member does not answer. The distribution algorithms, also configured per line group, specify how to select a line group member.
- During hunting, the hunt option, distribution algorithm, RNAR timeout, the maximum hunt timer, and final forwarding settings are considered.
- Call hunting implementation includes configuration of IP phone lines, line groups, hunt lists, and hunt pilots.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-34

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager Administration Guide Release 6.0(1)
[http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfg/bccm.pdf](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf)
- Cisco Unified Communications Manager System Guide Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmsys/accm.pdf
- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- MGCP gateway integration in Cisco Unified Communications Manager features automatic gateway configuration by using a Cisco Unified Communications Manager TFTP configuration server.
- Cisco Unified Communications Manager call routing is based on a best-match logic of the dialed number; path selection is performed based on route lists and route groups.
- Digit manipulation in Cisco Unified Communications Manager can be performed at several configuration elements such as translation patterns, route patterns, and route lists.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-1

Module Summary (Cont.)

- Cisco Unified Communications Manager uses partitions and CSS, and other configuration elements such as time periods and time schedules, blocked patterns, and forced authorization codes for calling privilege implementation.
- Cisco Unified Communications Manager provides various ways of providing call coverage, including call forward settings, call pickup features, shared lines, and the implementation of complex call hunting algorithms.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—4-2

This module describes how to enable Cisco Unified Communications Manager for public switched telephone network (PSTN) calls and how to implement a dial plan for internal and external calls in a single-site environment. The module first describes how to implement Media Gateway Control Protocol (MGCP) gateways for PSTN access. Then the module describes how call routing decisions are made in Cisco Unified Communications Manager based on dialed digits, and how path selection is performed after an entry in the call routing table is found. The module then covers digit manipulation options in Cisco Unified Communications Manager, followed by a discussion of calling privilege implementation. Several examples on how to use the available calling privilege configuration elements to implement classes of service or to perform routing decisions based on the calling device are shown. Finally, the module provides an overview of call coverage features with a detailed discussion on how to implement call hunting in Cisco Unified Communications Manager.

References

For additional information, refer to these resources:

- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
[http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfg/bccm.pdf](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf)
- Cisco CallManager and Cisco IOS Interoperability Guide – Configuring MGCP Gateway Support for Cisco Unified Communications Manager
http://www.cisco.com/en/US/partner/products/ps6441/products_configuration_guide_chapter09186a00805583bd.html
- Cisco Unified Communications Manager Dial Plan Deployment Guide
http://www.cisco.com/en/US/products/sw/voicesw/ps5629/prod_maintenance_guides_list.html
- Cisco Unified Communications Manager System Guide Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmsys/accm.pdf

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) Which of these protocols is an RFC-standardized master/slave protocol that is used to control voice gateways? (Source: Implementing MGCP Gateways in Cisco Unified Communications Manager)
- A) H.323
 - B) SIP
 - C) MGCP
 - D) SCCP
- Q2) Which two of the following are features that are supported for MGCP gateways in Cisco Unified Communications Manager? (Choose two.) (Source: Implementing MGCP Gateways in Cisco Unified Communications Manager)
- A) auto-registration
 - B) configuration server
 - C) PRI backhauling
 - D) dynamic dial peers
- Q3) Which two of these tasks are *not* MGCP gateway configuration tasks in Cisco Unified Communications Manager? (Choose two.) (Source: Implementing MGCP Gateways in Cisco Unified Communications Manager)
- A) Add the MGCP gateway.
 - B) Configure the IP address of the gateway.
 - C) Configure voice modules.
 - D) Configure voice interface cards.
 - E) Add the gatekeeper.
- Q4) Which two of these commands are required at the Cisco IOS MGCP gateway as a minimum? (Choose two.) (Source: Implementing MGCP Gateways in Cisco Unified Communications Manager)
- A) **mgcp call-agent (IP address of call agent)**
 - B) **ccm-manager config**
 - C) **mgcp**
 - D) **ccm-manager config (IP address of configuration server)**
 - E) **ccm-manager mgcp**
- Q5) Which definition best describes off-net dialing? (Source: Configuring Cisco Unified Communications Manager Call Routing Components)
- A) calls that originate and terminate on the same telephony network
 - B) use of internal number to reach a PSTN phone
 - C) calls that originate from one telephony network and terminate on a different telephony network
 - D) use of speed dials to reach an internal phone

- Q6) Which two of the following are *not* entries in the call routing table of Cisco Unified Communications Manager? (Choose two.) (Source: Configuring Cisco Unified Communications Manager Call Routing Components)
- A) directory numbers
 - B) translation pattern
 - C) trunk
 - D) route pattern
 - E) hunt pilot
 - F) call park numbers
 - G) Meet-Me numbers
 - H) gateway
- Q7) Which two methods of digit collection are not supported in Cisco Unified Communications Manager? (Choose two.) (Source: Configuring Cisco Unified Communications Manager Call Routing Components)
- A) SCCP en bloc
 - B) SCCP overlap sending and receiving
 - C) SCCP digit-by-digit.
 - D) SIP en bloc
 - E) SIP digit-by-digit using KPML
- Q8) Which statement describes call routing? (Source: Configuring Cisco Unified Communications Manager Call Routing Components)
- A) Call routing is the process of finding an entry in the call routing table that matches the dialed number.
 - B) Call routing is the process of selecting the device where the call is sent to.
 - C) Call routing is the process of finding an entry in the call routing table that matches the called number.
 - D) Call routing is the process of sending VoIP RTP packets towards the destination of the call.
- Q9) Which of the following is *not* a path selection configuration step? (Source: Configuring Cisco Unified Communications Manager Call Routing Components)
- A) Add gateways and trunks.
 - B) Build route groups from available devices.
 - C) Build route lists from available route groups.
 - D) Build route patterns pointing to route groups.
- Q10) Which statement does *not* apply to urgent priority? (Source: Configuring Cisco Unified Communications Manager Call Routing Components)
- A) Urgent priority can be configured at route patterns and translation patterns.
 - B) Urgent priority is used to force immediate routing as soon as a match is detected—even if other, longer route patterns are potential matches.
 - C) Urgent priority is often used with emergency numbers.
 - D) A pattern with urgent priority effectively excludes the urgent pattern from a longer route pattern range.

- Q11) Which of the following allows called and calling numbers to be modified during call processing? (Source: Implementing Cisco Unified Communications Manager Digit Manipulation)
- A) the use of calling search spaces
 - B) digit randomization
 - C) digit collection
 - D) digit manipulation
- Q12) Which two types of digit manipulation are commonly required on outgoing PSTN calls? (Choose two.) (Source: Implementing Cisco Unified Communications Manager Digit Manipulation)
- A) removing the PSTN access code from the calling party number
 - B) removing the PSTN access code from the called party number
 - C) expanding the calling party number to an E.164 number
 - D) expanding the called party number to an E.164 number
 - E) adding the PSTN access code to the calling party number
 - F) adding the PSTN access code to the called party number
- Q13) Which of the following is *not* a digit manipulation configuration element? (Source: Implementing Cisco Unified Communications Manager Digit Manipulation)
- A) external phone number mask
 - B) prefix
 - C) transformation masks
 - D) Call Forward All Destination
 - E) translation pattern
 - F) significant digits
- Q14) Which digit manipulation feature is configured at the directory number but enabled as part of the calling party transformation settings? (Source: Implementing Cisco Unified Communications Manager Digit Manipulation)
- A) external phone number mask
 - B) prefix
 - C) translation pattern
 - D) significant digits true
- Q15) Which two discard digits instructions are the only ones available for route patterns that do not use the @ sign? (Choose two.) (Source: Implementing Cisco Unified Communications Manager Digit Manipulation)
- A) PreAt
 - B) 11D->10D
 - C) NoDigits
 - D) Intl TollBypass
 - E) PreDot
- Q16) Which two statements are correct about transformation masks? (Choose two.) (Source: Implementing Cisco Unified Communications Manager Digit Manipulation)
- A) They can be used to modify either the calling number or called number.
 - B) They can contain digits 0-9, *, #, and X.
 - C) They are part of the calling and called party transformations settings.
 - D) They can only be applied to the called party number.
 - E) They are configured only at translation patterns.

- Q17) If a call routing lookup matches a _____, the translated called number is looked up again in the call routing table. (Source: Implementing Cisco Unified Communications Manager Digit Manipulation)
- A) translation pattern
 - B) route pattern
 - C) transformation mask
 - D) transformation pattern
- Q18) Which statement about significant digits is correct? (Source: Implementing Cisco Unified Communications Manager Digit Manipulation)
- A) They are configurable at gateways and trunks and apply to the calling party number.
 - B) They are configurable at route patterns and apply to both, the called and the calling party number.
 - C) They are configurable at gateways and trunks and apply to the called party number.
 - D) They are configurable at translation patterns and apply to the called party number on incoming calls only.
- Q19) What is the correct order of digit manipulation on the called number of outgoing calls? (Source: Implementing Cisco Unified Communications Manager Digit Manipulation)
- A) discard digits instructions, transformation mask, prefix digits, external phone number mask
 - B) discard digits instructions, transformation mask, prefix digits
 - C) discard digits instructions, prefix digits, transformation mask
 - D) transformation mask, external phone number mask, discard digits instructions, prefix digits
- Q20) Which statement describes what calling privileges are used for? (Source: Implementing Calling Privileges in Cisco Unified Communications Manager)
- A) Calling privileges are used to prioritize important calls over less important calls.
 - B) Calling privileges are used to control telephony charges.
 - C) Calling privileges give priority to voice over data.
 - D) Calling privileges give priority to on-net calls versus off-net calls.
-
- Q21) Which two statements are true about partitions and calling search spaces? (Choose two.) (Source: Implementing Calling Privileges in Cisco Unified Communications Manager)
- A) When two devices are in the same partition, they can call each other.
 - B) When two devices have the same calling search space, they can call each other.
 - C) A device has only access to those numbers that are in partitions listed in the calling device's calling search space.
 - D) If a number is in no partition, it is accessible by all devices.
 - E) If a device has no calling search space, it has access to all devices.

- Q22) Which configuration element is *not* used to implement time-of-day routing? (Source: Implementing Calling Privileges in Cisco Unified Communications Manager)
- A) time schedules
 - B) time periods
 - C) partitions
 - D) time range
- Q23) Which feature allows calls to be permitted or denied based on end user authorization? (Source: Implementing Calling Privileges in Cisco Unified Communications Manager)
- A) CMC
 - B) FAC
 - C) ACL
 - D) CDR
- Q24) Which of the following is *not* an example of an application of calling privileges? (Source: Implementing Calling Privileges in Cisco Unified Communications Manager)
- A) emergency calls
 - B) PLAR
 - C) time of day-based carrier selection
 - D) CDR
- Q25) What is the advantage of the line/device approach when implementing calling search spaces? (Source: Implementing Calling Privileges in Cisco Unified Communications Manager)
- A) If a phone has multiple lines, a single device CSS can be configured at the device, which is applicable to all lines. Only lines that need different configuration need to be configured with a line CSS which will overwrite the device CSS.
 - B) It scales better when implementing class of service and gateway selection.
 - C) It scales better when applying class of service to phones with more than one line.
 - D) It allows a different CSS to be used on outgoing versus incoming calls.
- Q26) Which two of the following steps are *not* required when implementing vanity numbers? (Choose two.) (Source: Implementing Calling Privileges in Cisco Unified Communications Manager)
- A) Create a site-specific partition for each physical location.
 - B) Create a service-specific partition for each different service.
 - C) For each service, configure the same vanity number once per physical location.
 - D) Apply site-specific partitions to the configured vanity numbers.
 - E) Put the appropriate site-specific partition into the CSS of the phones.
 - F) Put the appropriate service-specific partition into the CSS of the phones.
- Q27) Which two configuration elements are *not* used to implement time of day-based carrier selection? (Choose two.) (Source: Implementing Calling Privileges in Cisco Unified Communications Manager)
- A) partitions with time schedules referring to time periods
 - B) calling search spaces
 - C) multiple route patterns containing different carrier codes
 - D) multiple identical route patterns with different digit manipulation
 - E) calling search spaces with time schedules referring to time periods

- Q28) Which two statements are correct about PLAR? (Choose two.) (Source: Implementing Calling Privileges in Cisco Unified Communications Manager)
- A) PLAR utilizes a null-string translation pattern.
 - B) PLAR is configured at the directory number.
 - C) PLAR requires a different partition per PLAR destination number.
 - D) PLAR is configured at route patterns.
 - E) PLAR requires that the phone have a CSS that only provides access to the PLAR destination number
- Q29) Which two of the following are no call coverage features? (Choose two.) (Source: Implementing Call Coverage in Cisco Unified Communications Manager)
- A) Call Forward
 - B) auto-registration
 - C) shared lines
 - D) Call Pickup
 - E) Call Admission Control
- Q30) Which of the following features can be configured at the IP phone? (Source: Implementing Call Coverage in Cisco Unified Communications Manager)
- A) Call Forward All
 - B) Call Forward Unregistered
 - C) Call Forward No Answer
 - D) Call Forward Busy
- Q31) Which two of the following are no call hunting configuration elements? (Choose two.) (Source: Implementing Call Coverage in Cisco Unified Communications Manager)
- A) shared lines
 - B) pickup groups
 - C) line groups
 - D) hunt lists
 - E) hunt pilots
- Q32) Which two statements are correct about hunt options and distribution algorithms? (Choose two.) (Source: Implementing Call Coverage in Cisco Unified Communications Manager)
- A) The hunt option specifies the order in which line group members are hunted.
 - B) The distribution algorithm specifies how the maximum hunt time is calculated based on the amount of line group members.
 - C) The hunt option specifies how to continue hunting based on the result of the last attempt.
 - D) The hunt option is configured at the hunt pilot; the distribution algorithm is configured at the hunt list.
 - E) The distribution algorithm specifies the order in which line group members are hunted.
- Q33) What is *not* a reason for hunting to stop? (Source: Implementing Call Coverage in Cisco Unified Communications Manager)
- A) A maximum hunt time expired.
 - B) The maximum number of hunt attempts is reached.
 - C) The hunt option was configured to stop hunting.
 - D) Hunt exhaustion (no more line group members to try).

- Q34) When personal preference is used for final forwarding, where is the call routed to after hunting fails? (Source: Implementing Call Coverage in Cisco Unified Communications Manager)
- A) to the call forward no coverage destination configured at the hunt pilot
 - B) to the call forward no coverage destination configured at the hunt list
 - C) to the call forward no coverage destination configured at the phone that forwarded the call to the hunt pilot
 - D) to the personal voice-mail box of the phone that forwarded the call to the hunt pilot

Module Self-Check Answer Key

- Q1) C
- Q2) B, C
- Q3) B, E
- Q4) B, D
- Q5) C
- Q6) C, H
- Q7) A, B
- Q8) A
- Q9) D
- Q10) A
- Q11) D
- Q12) B, C
- Q13) D
- Q14) A
- Q15) C, E
- Q16) D, E
- Q17) A
- Q18) C
- Q19) B
- Q20) B
- Q21) C, D
- Q22) D
- Q23) B
- Q24) D
- Q25) B
- Q26) B, F
- Q27) C, E
- Q28) A, C
- Q29) B, E
- Q30) A
- Q31) A, B
- Q32) C, E
- Q33) B
- Q34) C

Module 5

Implementation of Media Resources, Features, and Applications

Overview

A Cisco Unified Communications solution provides access to a broad range of easy-to-use features that enhance user productivity and communication. Cisco Unified Communications Manager not only offers numerous enterprise telephony features, but also natively includes features such as presence-enabled speed dials and call lists, simple integration with externally provided hardware media resources, voice-mail integration, and support for video calls.

This module describes types of media resources supported by Cisco Unified Communications Manager, how to configure software-based media resources provided by Cisco Unified Communications Manager servers, and how to implement Cisco hardware media resources. The module describes a selection of user features, such as the new intercom feature, phone services, and user web pages. Presence features that are natively supported by Cisco Unified Communications Manager are discussed, as well as voice-mail integration and Cisco Unified Video Advantage.

Module Objectives

Upon completing this module, you will be able to implement Cisco Unified Communications Manager media resources, configure features, integrate Cisco Unified Communications Manager with a voice-mail system, and implement Cisco Unified Video Advantage. This ability includes being able to meet these objectives:

- Describe Cisco Unified Communications Manager media resources, including conferences, transcoders, MTP, MOH, and annunciator services
- Describe and configure Cisco Unified Communications Manager user features
- Describe and configure presence-enabled speed dials and lists

- Integrate Cisco Unified Communications Manager with voice-mail systems and set up basic voice-mail functionality
- Implement Cisco Unified Video Advantage to allow video telephony calls being placed from Cisco IP phones

Lesson 1

Implementing Media Resources

Overview

This lesson describes available hardware and software media resources and how they are configured in Cisco Unified Communications Manager to provide features such as conferences, transcoding, media termination, and music on hold. It also explains how to perform access control to media resources using media resource groups and media resource group lists.

Objectives

Upon completing this lesson, you will be able to describe Cisco Unified Communications Manager media resources, including conferences, transcoding and Media Termination Point (MTP), music on hold (MOH), and annunciator services. This ability includes being able to meet these objectives:

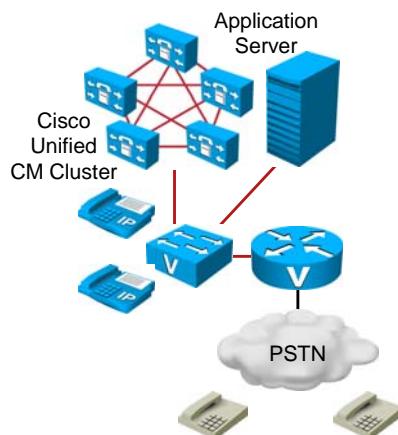
- Describe media resources
- Describe how Cisco Unified Communications Manager supports media resources
- Describe conferencing
- Configure conferencing media resources
- Configure Meet-Me conferences
- Describe MOH
- Configure MOH
- Describe Annunciator
- Describe Media Resources Access Control
- Configure Media Resources Access Control

Understanding Media Resources

This topic describes the different types of media resources and their usage in the Cisco Unified Communications Manager environment.

Types of Media Resources

- Voice termination
- Audio conferencing
- Transcoding
- Media Termination Point
- Annunciator
- Music on hold



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-4

A media resource is a software-based or hardware-based entity that performs media processing functions on the data streams to which it is connected. Media processing functions include mixing multiple streams to create one output stream (conferencing), passing the stream from one connection to another (Media Termination Point), converting the data stream from one compression type to another (transcoding), echo cancellation, signaling, termination of a voice stream from a time-division multiplexing (TDM) circuit (coding/decoding), packetization of a stream, streaming audio (annunciation), and so forth.

Not all of the different media resources are needed in every deployment. Required resources can be provided by software-based features, or digital signal processors (DSPs) have to be provisioned to implement the resources. The same basic resources (DSPs and Cisco IP Voice Media Streaming Application) may be shared to implement higher-level functions.

Media Resources Functions

This subtopic describes the functions of media resources.

Media Resources Functions

	Function
Voice termination	TDM legs must be terminated by hardware that performs coding/decoding and packetization of the stream. This is performed DSP resources residing in the hardware module.
Audio Conferencing	A conference bridge joins multiple participants into a single call. It mixes the streams together and creates a unique output stream for each connected party.
Transcoding	A transcoder converts an input stream from one codec into an output stream that uses a different codec.
Media Termination Point (MTP)	An MTP bridges the media streams together and allows them to be set up and torn down independently.
Annunciator	An annunciator streams spoken messages and various call progress tones.
Music on Hold	MOH provides music to callers when their call is placed on hold, transferred, parked, or added to a conference.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-5

The media resources in Cisco Unified Communications Manager and their functions are described as follows:

- **Voice termination:** Applies to a call that has two call legs, one leg on a TDM interface and the second leg on a VoIP connection. The TDM leg must be terminated by hardware that performs coding/decoding and packetization of the stream.
This termination function is performed by DSP resources residing in the same hardware module, blade, or platform. All DSP hardware on Cisco TDM gateways is capable of terminating voice streams, and certain hardware is also capable of performing other media resource functions such as conferencing or transcoding.
- **Conference bridge:** A resource that joins multiple participants into a single call. It can accept any number of connections for a given conference, up to the maximum number of streams allowed for a single conference on that device. There is a one-to-one correspondence between media streams connected to a conference and participants connected to the conference. The conference bridge mixes the streams together and creates a unique output stream for each connected party. The output stream for a given party is the composite of the streams from all connected parties minus their own input stream. Some conference bridges mix only the three loudest talkers on the conference and distribute that composite stream to each participant minus their own input stream if they are one of the talkers.
- **Transcoder:** Takes the stream of one codec and converts it from one compression type to another compression type. For example, it could take a stream from a G.711 codec and transcode it in real time to a G.729 stream. In addition, a transcoder provides MTP capabilities and may be used to enable supplementary services for H.323 endpoints when required.

Two streams that use the same codec but with a different sampling rate may also be connected.

A single-site deployment usually has no need for transcoding devices.

- **Media Termination Point:** An entity that accepts two full-duplex G.711 streams. It bridges the media streams together and allows them to be set up and torn down independently. The streaming data received from the input stream on one connection is passed to the output stream on the other connection, and vice versa.
- **Annunciator:** A software function of the Cisco IP Voice Media Streaming Application that provides the ability to stream spoken messages or various call progress tones from the system to a user. It is capable of sending multiple one-way Real-Time Transport Protocol (RTP) streams to devices such as Cisco IP phones or gateways, and it uses Skinny Client Control Protocol (SCCP) messages to establish the RTP stream. The announcements may be customized by replacing the appropriate .wav file.
- **Music on Hold (MOH):** An integral feature of the Cisco Unified Communications system. This feature provides music to callers when their call is placed on hold, transferred, parked, or added to an ad hoc conference. Implementing MOH is relatively simple but requires a basic understanding of unicast and multicast traffic, MOH call flows, configuration options, and server behavior and requirements.

Cisco Unified Communications Manager Media Resources Support

This topic describes hardware- and software-based media resources.

Media Resource Matrix

	Software	Hardware
Voice Termination	No	Yes
Audio Conferencing	Yes	Yes
Transcoding	No	Yes
Media Termination Point	Yes	Yes
Annunciator	Yes	No
Music on Hold	Yes	No*

*SRST MOH supported

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-7

Cisco Unified Communications Manager offers software-based media resources. You can start the Cisco IP Voice Media Streaming Application to activate the following media resources:

- Audio conferencing
- Media Termination Point
- Annunciator
- Music on hold

The following media resources are only available in hardware:

- Transcoding
- Voice termination

Audio conferencing and Media Termination Point media resources can also be offered by hardware media resources. MOH is a special case; it only works in remote sites in the Survivable Remote Site Telephony (SRST) mode of a router.

Media Resource Signaling and Audio Streams

All media resources to be used must register with the Cisco Unified Communications Manager.

Media Resource Signaling and Audio Streams

- All media resources register with the Cisco Unified Communications Manager.
- Signaling between hardware media resources and Cisco Unified Communications Manager uses Cisco Skinny Client Control Protocol (SCCP).
- Audio streams are always terminated by media resources.
- There are no direct IP phone-to-IP phone audio streams if a media resources are involved.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-8

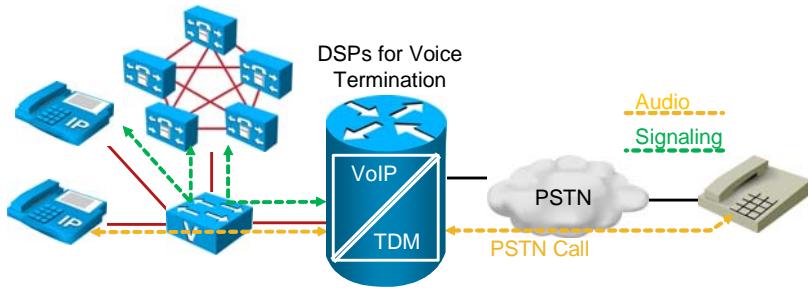
Signaling between external (hardware) media resources and Cisco Unified Communications Manager usually uses the Cisco SCCP.

All audio streams from any endpoint are always terminated by the media resources involved in the call. That means that there are no direct IP phone-to-IP phone audio streams if a media resource is involved in the call flow.

Voice Termination Signaling and Audio Streams

This subtopic describes voice termination signaling and audio streams in Cisco Unified Communications Manager.

Voice Termination Signaling and Audio Streams



- Voice termination applies to a call with a TDM and a VoIP call leg.
- TDM leg is terminated by hardware (coding/decoding, packetization).
- Termination is performed by DSPs installed in the gateway.
- Signaling occurs between gateway and Unified CM and between phone and Unified CM.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-9

The voice termination function is needed when an incoming or outgoing TDM call is created using a gateway. The TDM leg is terminated by the Cisco IOS router hardware and has to perform decoding, coding, and packetization functions. These functions are performed using hardware DSPs installed in the gateway.

There are two different audio streams, one inside the public switched telephone network (PSTN), the other a VoIP audio stream using RTP.

Signaling messages are exchanged between a gateway and Cisco Unified Communications Manager and between an IP phone and Cisco Unified Communications Manager. The PSTN signaling is not considered in the figure.

Audio Conferencing Signaling and Audio Streams

This subtopic describes audio conferencing signaling and audio streams in Cisco Unified Communications Manager.

Audio Conferencing Signaling and Audio Streams

The diagram illustrates the architecture of audio conferencing. It shows multiple IP phones connected to a central Integrated Conference Bridge. A gateway (GW) connects the conference bridge to the PSTN. Dashed arrows indicate the flow of audio and signaling between the phones, the bridge, and the gateway.

- A conference bridge joins multiple participants into a single call.
- Audio streams exist between IP phones and conference bridge and between gateway and conference bridge.
- Signaling occurs between IP phones and Unified CM, between conference bridge and Unified CM, and between gateway and Unified CM.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-10

A conference bridge joins multiple participants into a single call. The software conference bridge runs on one or more Cisco Unified Communications Manager servers in a cluster.

Audio streams exist between IP phones and a conference bridge and between a gateway and a conference bridge.

Signaling messages are exchanged between IP phones and Cisco Unified Communications Manager, between conference bridges and Cisco Unified Communications Manager, and between a gateway and Cisco Unified Communications Manager.

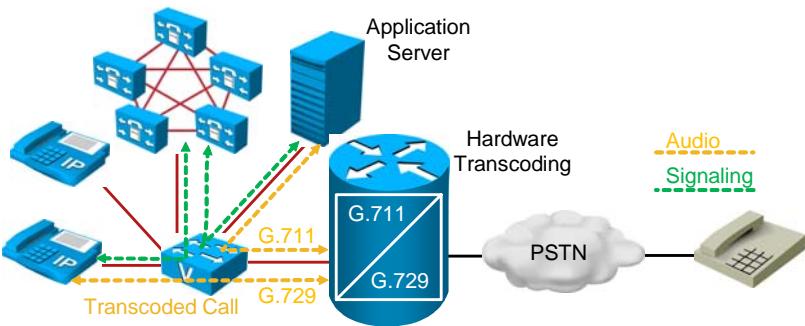
All conference bridges that are under the control of Cisco Unified Communications Manager use SCCP to communicate with Cisco Unified Communications Manager. Cisco Unified Communications Manager does not distinguish between software- and hardware-based conference bridges when it processes a conference allocation request.

The number of individual conferences that may be supported by the resource varies, and the maximum number of participants in a single conference varies, depending on the resource.

Transcoder Signaling and Audio Streams

This subtopic describes transcoder signaling and audio streams in Cisco Unified Communications Manager.

Transcoding Signaling and Audio Streams



- A transcoder converts streams from one codec into another.
- The transcoder in the example above runs in the Cisco IOS router.
- Audio streams exist between IP phones and transcoder and between application server and transcoder.
- Signaling occurs between IP phones and Unified CM, between transcoder and Unified CM, and between application server and Unified CM.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-11

A transcoder converts an input audio stream using one codec into an output stream that uses a different codec. The transcoder in the example is implemented using the Cisco IOS router DSP resources. The example is about an application server, such as a voice-mail server that only supports G.711 codecs, but in the Cisco Unified Communications Manager network, the G.729 codec is preferred.

Audio streams exist from the IP phones to the transcoder and from the application server to the transcoder.

Signaling messages are exchanged between IP phones and Cisco Unified Communications Manager, between a transcoder and Cisco Unified Communications Manager, and between an application server and Cisco Unified Communications Manager.

DSP resources are required to perform transcoding. Those DSP resources can be located in the voice modules and the hardware platforms for transcoding.

MTP Signaling and Audio Streams

This subtopic describes MTP signaling and audio streams in Cisco Unified Communications Manager.

Media Termination Point Signaling and Audio Streams

- The MTP bridges two media streams together and allows them to be set up and torn down independently.
- Audio streams exist between IP phones and MTP.
- Signaling is exchanged between IP phones and Cisco Unified Communications Manager, and between MTP and Cisco Unified Communications Manager.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-12

The MTP bridges two media streams together and allows them to be set up and torn down independently.

An MTP can be used as an instance of translation between incompatible audio streams, to synchronize clocking, or to enable certain devices for supplementary services.

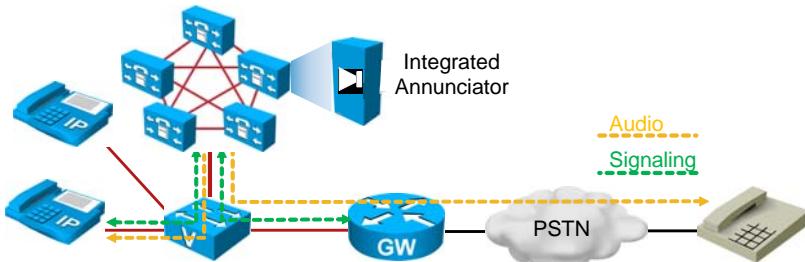
Audio streams exist between IP phones and MTP.

Signaling messages are exchanged between IP phones and Cisco Unified Communications Manager and between MTP and Cisco Unified Communications Manager.

Annunciator Signaling and Audio Streams

This subtopic describes annunciator signaling and audio streams in Cisco Unified Communications Manager.

Annunciator Signaling and Audio Streams



- Annunciator streams spoken messages and various call progress tones.
- Audio streams exist between IP phones and annunciator and between gateway and annunciator.
- Signaling is exchanged between IP phones and Unified CM, between the annunciator and Unified CM, and between the gateway and Unified CM.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-13

An annunciator is a software function of the Cisco IP Voice Media Streaming Application that provides the ability to stream spoken messages or various call progress tones from the system to a user.

It is capable of sending multiple one-way RTP streams to devices such as Cisco IP phones or gateways, and it uses SCCP messages to establish the RTP stream. The device must be capable of SCCP to use this feature. Tones and announcements are predefined by the system. The announcements support localization and also may be customized by replacing the appropriate .wav file. The annunciator is capable of supporting G.711 a-law and mu-law, G.729, and wideband codecs without any transcoding resources.

Signaling messages are exchanged between IP phones and Cisco Unified Communications Manager, between the annunciator and Cisco Unified Communications Manager, and between the gateway and Cisco Unified Communications Manager.

The audio stream is only one-way, from the annunciator to the IP phone or the gateway.

MOH Signaling and Audio Streams

This subtopic describes MOH signaling and audio streams in Cisco Unified Communications Manager.

Music on Hold Signaling and Audio Streams

- The MOH feature provides music to callers when their call is placed on hold, transferred, parked, or added to a conference.
- Audio streams exist between IP phones and MOH server and between gateway and MOH server.
- Signaling is exchanged between IP phones and Unified CM, between the MOH server and Unified CM, and between the gateway and Unified CM.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-14

MOH is an integral feature of the Cisco Unified Communications system. This feature provides music to callers when their call is placed on hold, transferred, parked, or added to an ad hoc conference. Implementing MOH is relatively simple but requires a basic understanding of unicast and multicast traffic, MOH call flows, configuration options, and server behavior and requirements.

Audio streams exist between IP phones and the MOH server and between the gateway and the MOH server.

Signaling messages are exchanged between IP phones and Cisco Unified Communications Manager, between the MOH Server and Cisco Unified Communications Manager, and between the gateway and Cisco Unified Communications Manager.

Conferencing Resources

This topic describes conferencing resources in the Cisco Unified Communications Manager environment.

Audio Conferencing Media Resources

The diagram illustrates the architecture of audio conferencing media resources. It shows several blue icons representing IP phones connected to a central conference bridge. One path from the phones leads to a 'Software Conference Bridge in Unified CM Server'. Another path leads to a 'Hardware Conference Bridge in Cisco IOS Router'. A third path leads to a 'Hardware Conference Bridge in Switch Chassis (CMM-Module)'. All three paths converge at a central 'GW' (Gateway) node. From the GW, a line extends to a cloud icon labeled 'PSTN', which is connected to a traditional telephone icon.

- Unified CM supports hardware and software conference bridges.
- The software-based conference bridge only supports single-mode conferences, using the G.711 codec.
- Some hardware-based conference bridges support mixed-mode conferences with participants using different codecs.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-16

The Cisco Unified Communications Manager supports hardware and software conference bridges.

The software-based conference bridge, implemented as a Cisco Unified Communications Manager service, only supports single-mode conferences, using a single codec (G.711).

Some hardware conference bridges can support multiple low-bit-rate (LBR) stream types such as G.729, Global System for Mobile Communications (GSM), or G.723; this capability enables these hardware conference bridges to handle mixed-mode conferences. In a mixed-mode conference, the hardware conference bridge transcodes G.729, GSM, and G.723 streams into G.711 streams, mixes them, and then encodes the resulting stream into the appropriate stream type for transmission back to the user. Some hardware conference bridges support only G.711 conferences.

Software Audio Conferencing Bridge

A software unicast conference bridge is a standard conference mixer that is capable of mixing G.711 audio streams and Cisco wideband audio streams.

Software Audio Conferencing Bridge

- Part of Cisco IP Voice Media Streaming Application service.
- Software audio conference limitations.
 - Unicast audio streams only.
 - Any combination of G.711 a-law, G.711 mu-law, or wideband audio streams may be connected.
- The maximum number of audio streams is 128* per server.

	Minimum Participants	Maximum Participants	Default Participants
Ad Hoc	3	64	4
Meet-Me	1	128	4

*Maximum 48 participants when Cisco Unified Communications Manager service is activated.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-17

Any combination of wideband or G.711 a-law and mu-law streams may be connected to the same conference. The number of conferences that can be supported on a given configuration depends on the server on which the conference bridge software is running and on what other functionality has been enabled for the application. The Cisco IP Voice Media Streaming Application is a resource that can also be used for several functions, and the design must consider all functions.

Hardware Audio Conferencing

A hardware conference bridge has all the capabilities of a software conference bridge. In addition, some hardware conference bridges can support multiple LBR stream types such as G.729, GSM, or G.723.

Hardware Audio Conferencing

Cisco Unified Communications Manager Resource Type	Conferences Resource
Cisco Conference Bridge Hardware	WS-X6608-T1, WS-X6608-E1
Cisco IOS Conference Bridge	NM-HDV
Cisco Conference Bridge (WS-SVC-CMM)	WS-SVC-CMM
Cisco IOS Enhanced Conference Bridge	PVDM2, NM-HD, NM-HDV2
Cisco Video Conference Bridge (IPVC-35xx)	IP/VC-35xx

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-18

All conference bridges that are under the control of Cisco Unified Communications Manager use SCCP to communicate with Cisco Unified Communications Manager.

Cisco Unified Communications Manager allocates a conference bridge from a conferencing resource that is registered with the Cisco Unified Communications Manager cluster. Both hardware and software conferencing resources can register with Cisco Unified Communications Manager at the same time, and Cisco Unified Communications Manager can allocate and use conference bridges from either resource. Cisco Unified Communications Manager does not distinguish between these types of conference bridges when it processes a conference allocation request.

The number of individual conferences that may be supported by the resource varies, and the maximum number of participants in a single conference varies, depending on the resource.

The following types of hardware conference bridge resources may be used on a Cisco Unified Communications Manager system:

- Hardware Audio Conference Bridge (Cisco NM-HDV2, NM-HD-1V/2V/2VE, 2800 Series, and 3800 Series Routers)
- Hardware Audio Conference Bridge (Cisco WS-SVC-CMM-ACT)
- Hardware Audio Conference Bridge (Cisco NM-HDV and 1700 Series Routers)
- Hardware Audio Conference Bridge (Cisco Catalyst WS-X6608-T1 and WS-X6608-E1)

Conferences per Resource

Conferences per Resource

Conferences Resource	Participants per Resource (G.711/G.729)	Participants per Conference
WS-X6608-T1, WS-X6608-E1	32 per port 256 per module	6
NM-HDV (max. 5 PVDM-12, each 3 TI549 DSPs)	60 per NM	6
WS-SVC-CMM	64 per port adapter 256 per module	8
PVDM2, NM-HD, NM-HDV2	64 per DSP NM-HDV2 is limited to 400	8

- Impact secure conferencing:
 - Sessions capacity is reduced by half from that of nonsecure conference with G.711.
 - Number of conferees per session is the same as it was in nonsecure conference.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-19

The following guidelines and considerations apply to the DSP resources:

- Hardware Audio Conference Bridge (Cisco NM-HDV2, NM-HD-1V/2V/2VE, 2800 Series, and 3800 Series Routers)
 - Based on the C5510 DSP chipset, the NM-HDV2 and the router chassis use the PVDM2 modules for providing DSPs.
 - DSPs on PVDM2 hardware are configured individually as either voice termination, conferencing, media termination, or transcoding, so that DSPs on a single PVDM may be used as different resource types. Allocate DSPs to voice termination first, then to other functionality as needed.
 - The NM-HDV2 has four slots that will accept PVDM2 modules in any combination. The other network modules have fixed numbers of DSPs.
 - A conference based on these DSPs allows a maximum of eight participants. When a conference begins, all eight positions are reserved at that time.
 - The PVDM2-8 is listed as having one-half of a DSP because it has a DSP that has half the processing capacity of the PVDM2-16. For example, if the DSP on a PVDM2- 8 is configured for G.711, it can provide (0.5×8) bridges / DSP = 4 conference bridges.
 - A DSP farm configuration in Cisco IOS gateway specifies which codecs may be accepted for the farm. A DSP farm that is configured for conferencing and G.711 provides eight conferences. When configured to accept both G.711 and G.729 calls, a single DSP provides two conferences because it is also reserving its resources for performing transcoding of streams.

- The I/O of an NM-HDV2 is limited to 400 streams, so you must ensure that the number of conference resources allocated does not cause this limit to be exceeded. If G.711 conferences are configured, then no more than 6 DSPs (total of 48 conferences with 8 participants each) should be allocated per network module because $(48 * 8)$ participants = 384 streams. If all conferencing is configured for both G.711 and G.729 codecs, then each DSP provides only 2 conferences of 8 participants each. In this case, it is possible to populate the network module fully and configure it with 16 DSPs, so there would be 256 streams.
- Conferences cannot natively accept calls using the GSM codec. A transcoder must be provided separately for these calls to participate in a conference.
- Hardware Audio Conference Bridge (Cisco WS-SVC-CMM-ACT)
 - This Cisco Catalyst-based hardware provides DSP resources that may provide conference bridges of up to 32 participants per bridge.
 - Each module contains 4 DSPs that are individually configurable. Each DSP can support 32 conference bridges.
 - The G.711 and G.729 codecs are supported on these conference bridges without extra transcoder resources. However, transcoder resources would be necessary if other codecs are used.
- Hardware Audio Conference Bridge (Cisco NM-HDV and 1700 Series Routers)
 - This hardware uses the PVDM-256K-type modules that are based on the C549 DSP chipset. Conferences using this hardware provide bridges that allow up to six participants in a single bridge.
 - The resources are configured on a per-DSP basis as conference bridges.
 - The NM-HDV may have up to 4 PVDM-256K modules, while the Cisco 1700 Series Routers may have 1 or 2 PVDM-256K modules.
 - Each DSP provides a single conference bridge that can accept G.711 or G.729 calls.
 - The Cisco 1751 is limited to 5 conference calls per chassis, and the Cisco 1760 can support 20 conference calls per chassis.
 - Any PVDM2-based hardware, such as the NM-HDV2, may be used simultaneously in a single chassis for voice termination but may not be used simultaneously for other media resource functionality. The DSPs based on PVDM-256K and PVDM2 have different DSP farm configurations, and only one may be configured in a router at a time.
- Hardware Audio Conference Bridge (Cisco Catalyst WS-X6608-T1 and WS-X6608-E1)
 - This hardware has eight DSPs that are physically associated to each port, and there are eight ports per card.
 - Configuration of the DSPs is at the port level, so that all DSPs associated to a port perform the same function.
 - Conference bridges may have up to 32 participants, and each port supports 32 conference bridges.
 - For conferences with G.711 or G.723, there may be 32 conferences per port. If G.729 calls are used, there may be 24 conferences per port.

Built-In Conference Resource Characteristics

Some phone models have a built-in conference resource that allows a three-way conference.

Built-in Conference Resource Characteristics

- IP phones with built-in conference resources allow three-way conferences.
- Only invoked by Barge feature.
- G.711 support only.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-20

This built-in conference bridge is invoked only by the Barge feature and is not used as a general conferencing resource. This kind of bridge accepts only G.711 calls.

Meet-Me and Ad Hoc Conferencing Characteristics

Cisco Unified Communications Manager supports both Meet-Me conferences and ad hoc conferences.

Meet-Me and Ad Hoc Conferencing Characteristics

- Meet-Me
 - Allocate directory numbers
 - Manual distribution of Meet-Me number
 - No password-like access security to enter the conference
- Basic Ad Hoc
 - Conference originator controls the conference
 - Originator can add and remove participants
- Advanced Ad Hoc
 - Any participant can add and remove other participants
 - Link multiple ad hoc conferences together

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-21

Meet-Me conferences allow users to dial in to a conference. Ad hoc conferences allow the conference controller to add specific participants to the conference.

Meet-Me conferences require that a range of directory numbers be allocated for exclusive use of the conference. When a Meet-Me conference is set up, the conference controller chooses a directory number and advertises it to members of the group. The users call the directory number to join the conference. Anyone who has calling privileges to call the directory number while the conference is active can join the conference.

There are two types of ad hoc conferences: basic and advanced. In basic ad hoc conferencing, the originator of the conference acts as the controller of the conference and is the only participant who can add or remove other participants.

In advanced ad hoc conferencing, any participant can add or remove other participants; that capability does not get limited to the originator of the conference. Advanced ad hoc conferencing also allows linking multiple ad hoc conferences together. Set the Advanced Ad Hoc Conference Enabled cluster-wide service parameter to True to gain access to advanced ad hoc conferencing.

Conferencing Media Resource Configuration

This topic describes the configuration of conferencing media resources.

Conferencing Media Resource Configuration Steps

1. Configure software conference media resources (if desired)
 - a. Check if IP Voice Media Streaming Application service is running
 - b. Configure IP Voice Media Streaming Application service parameters
 - c. Check if software conferencing media resource exists
2. Implement hardware conference media resources (if desired)
 - a. Configure hardware media resource in Unified CM
 - b. Configure hardware media resource in Cisco IOS gateway
 - c. Check if the hardware media resource registered with Unified CM
3. Configure CallManager service parameters concerning conferencing

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-23

Three main steps are required to configure conferencing media resources, as shown in the figure.

Step 1a: Activate IP Voice Media Streaming Application Service

First, the Cisco IP Voice Media Streaming Application service needs to be activated.

Step 1a: Activate IP Voice Media Streaming Application Service

Service Activation

Select Server
Server* 10.1.1.1 Go Check All Services

CM Services		Activation Status
	Service Name	
<input checked="" type="checkbox"/>	Cisco CallManager	Activated
<input checked="" type="checkbox"/>	Cisco Tftp	Activated
<input type="checkbox"/>	Cisco Messaging Interface	Deactivated
<input type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Deactivated
<input type="checkbox"/>	Cisco IP Voice Media Streaming App	Deactivated
<input type="checkbox"/>	Cisco CTIManager	Deactivated
<input type="checkbox"/>	Cisco Extension Mobility	Deactivated
<input type="checkbox"/>	Cisco Extended Functions	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer	Deactivated
<input type="checkbox"/>	Cisco DHCP Monitor Service	Deactivated

Activate the IP Voice Media Streaming App service in Cisco Unified Serviceability under Service Activation to enable software media resources on Cisco Unified Communications Manager servers.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-24

You can activate the Cisco IP Voice Media Streaming Application service in Cisco Unified Serviceability under **Tools > Service Activation**. At the top of the service activation screen, choose the server on which services should be activated or deactivated. After choosing the server, click the check box at the IP Voice Media Streaming App service and click **Save**.

Step 1b: IP Voice Media Streaming Application Service Parameters

The next step is to configure the IP Voice Media Streaming Application service parameters.

Service Parameter Configuration

Select Server and Service

Server* 10.1.1.1 (Active)

Service* Cisco IP Voice Media Streaming App (Inactive)

All parameters apply only to the current server except parameters that are in the Clusterwide group(s).

Cisco IP Voice Media Streaming App (Inactive) Parameters on server 10.1.1.1 (Active)

Parameter Name	Parameter Value	Suggested
Announcer (ANN) Parameters		
Call Count *	48	48
Run Flag *	True	True
Conference Bridge (CFB) Parameters		
Call Count *	48	48
Run Flag *	True	True
Media Termination Point (MTP) Parameters		
Call Count *	48	48
Run Flag *	True	True

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-25

Cisco IP Voice Media Streaming Application service parameters concerning the software conference bridge are as follows:

- **Call Count:** This parameter specifies the maximum number of conference participants that the conference bridge will support. Increasing this value above the recommended default may cause performance degradation on a Cisco Unified Communications Manager that is running on the same server. If it is necessary to increase this value above the default, consider installing the Cisco IP Voice Media Streaming Application on a separate server. The range is 0 to 256, the default is 48.
- **Run Flag:** This parameter determines whether the conference bridge functionality of the Cisco IP Voice Media Streaming Application is enabled. Valid values are True (enabled) or False. The default is True.

Note	These settings are service parameters of the Cisco IP Voice Media Streaming Application service and can be accessed from Cisco Unified Communications Manager Administration under System > Service Parameters .
-------------	--

Step 1c: Software Conferencing Media Resource

The Cisco Unified Communications Manager conference resource is automatically added when the Cisco IP Voice Media Streaming App services are activated.

Step 1c: Software Conferencing Media Resource

Conference Bridge Configuration

Conference Bridge Information	
Conference Bridge :	CFB_2 (CFB_CUCM1-1)
Registration	Registered with Cisco Unified Communications Manager 10.1.1.1
IP Address	10.1.1.1
 Software Conference Bridge Info	
Conference Bridge Type*	Cisco Conference Bridge Software
Host Server	10.1.1.1
Conference Bridge Name*	<input type="text" value="CFB_2"/>
Description	<input type="text" value="CFB_CUCM1-1"/>
Device Pool*	<input type="text" value="Default"/>
Common Device Configuration	<input type="text" value="< None >"/>
Location*	<input type="text" value="Hub_None"/>

Conference bridge is automatically added with default configuration parameters when the IP Voice Media Streaming App service is activated.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-26

The figure shows the default configuration of a software conference resource. The only configurable items are Name, Description, Device Pool, Common Device Configuration, and Location.

Note

The Cisco Unified Communications Manager software conference media resource only supports the G.711 and wideband codecs. Use a transcoder to allow devices that use other codecs to participate in a conference, or use hardware conference resources that support additional codecs.

Step 2a: Configuration of Cisco IOS Enhanced Conference Bridge in Cisco Unified Communications Manager

The next step is to configure the Cisco IOS Enhanced Conference Bridge in Cisco Unified Communications Manager.

Step 2a: Configuration of a Cisco IOS Enhanced Conference Bridge in Unified CM

Conference Bridge Information

Conference Bridge :	CFB001b0cc250f8 (CFB001b0cc250f8)
Registration	Registered with Cisco Unified CallManager 172.47.1.111
IP Address	172.47.2.1

IOS Conference Bridge Info

Conference Bridge Type*	Cisco IOS Enhanced Conference Bridge
Conference Bridge Name*	CFB001b0cc250f8
Description	CFB001b0cc250f8
Device Pool*	Default
Common Device Configuration	< None >
Location*	Hub_None
Device Security Mode*	Non Secure Conference Bridge

Add a new conference resource:

- Add the Conference Bridge Name CFB<MAC>
- Specify the Device Pool (Region and Location)
- Set the Device Security Mode

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-27

Cisco Unified Communications Manager Conference Bridge, a software or hardware application, allows both ad hoc and Meet-Me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

The hardware model type for Conference Bridge contains specific MAC address and device pool information. Different conference bridge fields display in Cisco Unified Communications Manager Administration, depending on the conference bridge type that was chosen.

Navigate to **Media Resources > Conference Bridge** and click **Add New**. The Conference Bridge Configuration window displays. Enter the appropriate settings as described below and click **Save**. The window refreshes and displays the conference device that was added. To reset the conference bridge device and apply the changes, click **Reset**.

The fields in the Conference Bridge Configuration window are described as follows:

- **Conference Bridge Type:** Choose Cisco IOS Conference Bridge or Cisco IOS Enhanced Conference Bridge.

Note The differences of these hardware conference bridge resources have been discussed in the previous topic.

- **Conference Bridge Name:** Enter a name for the conference bridge. The name has to match the name of the conference media resource as configured at the Cisco IOS router (see next step).

Note	If the conference bridge type is Cisco IOS Conference Bridge, the name of the Cisco IOS conference media resource is Call Forward Busy (CFB) followed by the MAC address of the interface that is used for SCCP signaling. If the conference bridge type is Cisco IOS Enhanced Conference Bridge, any name for the conference bridge media resource can be configured at the Cisco IOS router. The name is case-sensitive; it has to exactly match the name of the conference media resource at the Cisco IOS router.
-------------	---

- **Device Pool:** Choose a device pool or choose Default.
- **Common Device Configuration:** Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH, which support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.
- **Location:** Choose the appropriate location for this conference bridge. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes.
- **Device Security Mode:** This field displays for Cisco IOS Enhanced Conference Bridge only. If you choose Non Secure Conference Bridge, the nonsecure conference establishes a TCP port connection to Cisco Unified Communications Manager on port 2000. Ensure that this setting matches the security setting on the conference bridge, or the call will fail. The Encrypted Conference Bridge setting supports the secure conference feature. Refer to the *Cisco Unified Communications Manager Security Guide* for secure conference bridge configuration procedures.

Step 2b and 2c: Configuration and Verification of Cisco IOS Enhanced Conference Bridge

The figure below shows an example for the configuration of a Cisco IOS Enhanced Conference Bridge.

Step 2b and 2c: Configuration and Verification of Cisco IOS Enhanced Conference Bridge

```
voice-card 0
  dspfarm
  dsp services dspfarm
  sccp local FastEthernet0/0.72
  sccp ccm 10.1.1.1 identifier 1 version 6.0
  sccp
    sccp ccm group 1
      associate ccm 1 priority 1
      associate profile 1 register CFB001B0CC250F8
    dspfarm profile 1 conference
      codec g711ulaw
      codec g711alaw
      codec g729ar8
      codec g729abr8
      maximum sessions 2
      associate application SCCP
      no shutdown
```

Source interface for registration
Unified CM to register with
CCM ID has to match
Name to register with at Unified CM
Profile ID has to match

For verification use:
`show sccp`
`show sccp ccm group 1`
`show dspfarm profile 1`

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-28

The table shows the commands for configuring a Cisco IOS Enhanced Conference Bridge.

Command	Command Function
dspfarm	Enables DSP farm service. Use in global configuration mode. This command is enabled by default.
dsp services dspfarm	Enables DSP farm services for a particular voice network module. Use in interface configuration mode.
sccp local	Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco Unified Communications Manager. Use in global configuration mode.
sccp ccm	Adds a Cisco Unified Communications Manager server to the list of available servers and sets various parameters—including IP address or Domain Name System (DNS) name, port number, and version number. Use in global configuration mode.
sccp	Enables the SCCP protocol and its related applications (transcoding and conferencing). Use in global configuration mode.
sccp ccm group	Creates a Cisco Unified Communications Manager group and enters SCCP Cisco Unified Communications Manager configuration mode. Use in global configuration mode.
associate ccm	Associates a Cisco Unified Communications Manager with a Cisco Unified Communications Manager group and establishes its priority within the group. Use in the SCCP Cisco Unified Communications Manager configuration mode.
associate profile	Associates a DSP farm profile with a Cisco Unified Communications Manager group. Use in SCCP Cisco Unified Communications Manager configuration mode.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services. Use in global configuration mode.
codec	Specifies call density and codec complexity based on a particular codec standard. Use in DSP interface DSP farm configuration mode.
associate application sccp	Associates SCCP to the DSP farm profile. Use in DSP farm profile configuration mode.
maximum sessions	Specifies the maximum number of sessions that are supported by the profile. Use in DSP farm profile configuration mode.
no shutdown	If you fail to no shut the DSP farm profile, it will display in the gateway, but fail to operate.

Tip The name specified in the Cisco IOS device must match exactly the name in the Cisco Unified Communications Manager; the names are case sensitive.

Note When configuring a Cisco IOS Enhanced Conference bridge any name can be configured with the **associate profile** command. When configuring a Cisco IOS conference bridge the name cannot be configured; it is CFB(MAC) where (MAC) is the MAC address of the interface that was specified at the **sccp local** command.

To verify the Cisco IOS media resource configuration, use the following **show** commands:

show sccp

SCCP Admin State: UP

Gateway IP Address: 10.1.1.101, Port Number: 2000

```

IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.1.1.1, Port Number: 2000
Priority: N/A, Version: 6.0, Identifier: 1
Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.1.1.1, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 1
Reported Max Streams: 16, Reported Max OOS Streams: 0
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: g729r8, Maximum Packetization Period: 60
Supported Codec: g729br8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30

show sccp ccm group 1
CCM Group Identifier: 1
Description: None
Binded Interface: NONE, IP Address: NONE
Associated CCM Id: 1, Priority in this CCM Group: 1
Associated Profile: 1, Registration Name: CFB001B0CC250F8
Registration Retries: 3, Registration Timeout: 10 sec
Keepalive Retries: 3, Keepalive Timeout: 30 sec
CCM Connect Retries: 3, CCM Connect Interval: 10 sec
Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
Signaling DSCP value: cs3, Audio DSCP value: ef

show dspfarm profile 1
Dspfarm Profile Configuration
Profile ID = 1, Service = CONFERENCING, Resource ID = 1
Profile Description :
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : SCCP Status : ASSOCIATED
Resource Provider : FLEX_DSPRM Status : UP
Number of Resource Configured : 2
Number of Resource Available : 2
Codec Configuration
Codec : g711ulaw, Maximum Packetization Period : 30 ,
Transcoder: Not Required
Codec : g711alaw, Maximum Packetization Period : 30 ,
Transcoder: Not Required
Codec : g729ar8, Maximum Packetization Period : 60 ,
Transcoder: Not Required

```

Codec : g729abr8, Maximum Packetization Period : 60 ,
Transcoder: Not Required

Codec : g729r8, Maximum Packetization Period : 60 ,
Transcoder: Not Required

Codec : g729br8, Maximum Packetization Period : 60 ,
Transcoder: Not Required

Step 3: CallManager Service Parameters Concerning Conferencing

This step enables you to tune the Cisco Unified Communications Manager media resources with CallManager Service Parameters concerning conferencing.

Step 3: Cisco CallManager Service Parameters Concerning Conferencing

- Suppress MOH to Conference Bridge (True)
- Drop Ad Hoc Conference
 - Never (default)
 - When conference controller leaves
 - When no On-Net parties remain in the conference
- Advanced Ad Hoc Conference Enabled (False)
- Non-linear Ad Hoc Conference Linking Enabled (False)
- Maximum Ad Hoc Conference (4)
- Maximum Meet Me Conference (4)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-29

You can configure the following CallManager service parameters concerning conferencing:

- **Suppress MOH to Conference Bridge:** This parameter determines whether MOH plays to a conference when a conference participant places the conference on hold. Valid values are True (the system does *not* play MOH to the conference when a conference participant presses the **Hold** button) or False. The default is True.
- **Drop Ad Hoc Conference:** This parameter determines how an ad hoc conference terminates. Valid values are as follows:
 - **Never** (default): The conference remains active after the conference controller hangs up, and after all on-net parties hang up. Choosing this option means that if on-net parties conference in off-net parties and then disconnect, the conference stays active between the off-net parties, which could result in potential toll fraud.
 - **When Conference Controller Leaves:** Terminates the conference when the conference controller hangs up or when the conference controller transfers, redirects, or parks the conference call and the retrieving party hangs up.
 - **When No On-Net Parties Remain in the Conference:** Terminate the conference when there are no on-net parties remaining in the conference.

- **Advanced Ad Hoc Conference Enabled:** This parameter determines whether advanced ad hoc conference features are enabled. Advanced ad hoc conference features include the ability for conference participants other than the conference controller to add new participants to an existing ad hoc conference, the ability for any non-controller conference participant to drop other participants from the conference via the Conflist and RmLstC softkey, and whether ad hoc conferences can be linked together using features such as conference, join, direct transfer, and transfer. Valid values are True (allow advanced ad hoc conference features) or False. Default is False.
- **Non-linear Ad Hoc Conference Linking Enabled:** This parameter determines whether more than two ad hoc conferences can be linked directly to an ad hoc conference in a non-linear fashion. Non-linear conference linking occurs when three or more ad hoc conferences are linked directly to one other ad hoc conference. Linear conferencing linking occurs when one or two ad hoc conferences are linked directly to one other ad hoc conference. For this parameter to work, the Advanced Ad Hoc Conference Enabled service parameter must be set to True. Valid values are True (allow non-linear conference linking so that three or more ad hoc conferences can be linked to a single other conference) or False. The default is False. The Advanced Ad Hoc Conference Enabled service parameter must be set to True for the Non-linear Ad Hoc Conference Linking Enabled service parameter to work.
- **Maximum Ad Hoc Conference:** This parameter specifies the maximum number of participants that are allowed in a single ad hoc conference. The value of this field depends on the capabilities of the software/hardware conference bridge. The maximum number of conference bridge participants for typical conference bridges follow:
 - Software Conference: 64
 - Cisco Catalyst WS-X6608: 16
 - Cisco Catalyst 4000: 16
 - NM-HDV: 6

Setting this value above the maximum capacity of the conference will result in failed entrance to a conference bridge if more ports are added than the specific conference bridge configuration allows. The range is 3 to 64, the default is 4.
- **Maximum Meet-Me Conference Unicast:** This parameter specifies the maximum number of participants that are allowed in a single Unicast Meet-Me conference. The value of this field depends on the capabilities of the software/hardware conference bridge; for example, a software conference bridge conferences up to 128 participants. When a conference is created, the system automatically reserves a minimum of 3 streams, so specifying a value less than 3 allows a maximum of 3 participants. The range is 1 to 128, the default it 4.

Note	These settings are service parameters of the Cisco CallManager service and can be accessed from System > Service Parameters .
-------------	---

Meet-Me Conference Configuration

This topic describes the configuration of a Meet-Me conference pattern.

Meet-Me Conference Configuration

1. All needed hardware and software conference resources have to be configured.
2. Meet-Me number or pattern has to be configured.
 - Meet-Me number range is part of the dial plan and must not overlap with other numbers.
 - To restrict access to specific Meet-Me numbers, use partitions and calling search spaces.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-31

To configure directory numbers for Meet-Me conferences, first, you must ensure that the necessary hardware and software conference media resources are configured and available.

Then, you must configure a Meet-Me number or pattern. When a pattern is configured, you can use the “X” wildcard to specify ranges. The Meet-Me number range is part of the dial plan and must not overlap with other numbers. Partitions and calling search spaces must be configured if access to specific Meet-Me numbers should be restricted.

Step 2: Configure a Meet-Me Number or Pattern

The next step is to configure a Meet-Me number or pattern.

Step 2: Configure a Meet-Me Number/Pattern

Meet-Me Number Configuration

Meet-Me Configuration

Directory Number or Pattern*	45XX
Description	Meet-Me Range
Partition	< None >
Minimum Security Level*	Non Secure

Add Meet-Me numbers or patterns.
In this case, 100 Meet-Me conference numbers are created.

Cisco Unified CM Administration: **Call Routing > Meet-Me Number/Pattern**

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-32

To add a number or number range used for Meet-Me conferences, go to Cisco Unified Communications Manager Administration, **Call Routing > Meet-Me Number/Pattern**, click **Add New** and configure the new pattern with the following data:

- **Directory Number or Pattern:** Enter a Meet-Me numbers or pattern or a range of numbers. To configure a range, the dash must appear within brackets and follow a digit; for example, to configure the range 1000 to 1050, enter 10[0-5]0.
- **Description:** Enter up to 30 alphanumeric characters for a description of the Meet-Me number or pattern.
- **Partition:** To use a partition to restrict access to the Meet-Me number or pattern, choose the desired partition from the drop-down list box.
To exclude restricted access to the Meet-Me number or pattern, choose **<None>** for the partition.

Note Make sure that the combination of Meet-Me number or pattern and partition is unique within the Cisco Unified Communications Manager cluster.

- **Minimum Security Level:** Choose the minimum Meet-Me conference security level for this Meet-Me number or pattern from the drop-down list box:
 - Choose **Authenticated** to block participants with nonsecure phones from joining the conference.
 - Choose **Encrypted** to block participants with authenticated or nonsecure phones from joining the conference.
 - Choose **Non Secure** to allow all participants to join the conference.

Note	In order to use conference security, the Cisco Unified Communications Manager cluster has to be enabled for secure mode. More information about security features in Cisco Unified Communications Manager is provided in the CIPT2 course.
-------------	--

MOH Essentials

This topic describes the MOH server and its capabilities.

Music on Hold Media Resources

The diagram shows a network topology for MOH delivery. At the top, a blue rectangular box labeled "Integrated Software MOH Server in Unified CM Server" has arrows pointing down to four blue IP phone icons. These phones are connected to a central blue switch. Another blue rectangular box labeled "MOH as Multicast Stream from External Media Streaming Server" also has an arrow pointing down to the same four phones. Below the switch, there is a blue circle labeled "GW" (Gateway). A red line connects the switch to the GW. From the GW, a line goes to a white cloud-like shape labeled "PSTN". Finally, a grey telephone icon is connected to the PSTN.

- Unified CM uses an integrated software Music on Hold server.
- For special cases, external media streaming servers can be used.
- The Unified CM integrated Music on Hold server supports multicast and unicast for MOH streaming.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-34

For callers to hear MOH, Cisco Unified Communications Manager must be configured to support the MOH feature. The MOH feature has two main requirements:

- An MOH server to provide the MOH audio stream sources
- Cisco Unified Communications Manager configured to use the MOH streams provided by the MOH server when a call is placed on hold

The integrated MOH feature makes music available to any on-net or off-net device placed on hold. On-net devices include station devices and applications placed on hold, consult hold, or park hold by an interactive voice response (IVR) or call distributor. Off-net users include those connected through Media Gateway Control Protocol (MGCP), session initiation protocol (SIP), and H.323 gateways. The MOH feature is also available for plain old telephone service (POTS) phones connected to the Cisco IP network through Foreign Exchange Station (FXS) ports. The integrated MOH feature includes media server, database administration, call control, media resource manager, and media control functional areas. The MOH server provides the music resources and streams.

In special cases, you can configure multicast MOH streaming so that external media servers can be used to provide the MOH stream. Cisco Unified Communications Manager Express and Cisco Unified Survivable Remote Site Telephony (SRST) gateways can be configured as media streaming servers for MOH, by streaming audio files stored in the flash memory of Cisco IOS routers using multicast. For detailed information on this feature, consult the Cisco Unified Communications Solution Reference Network Design (SRND).

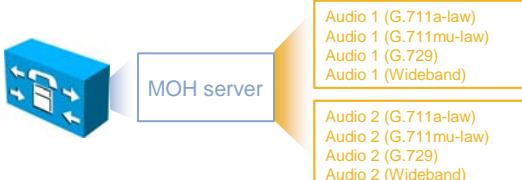
The Cisco Unified Communications Manager integrated MOH server supports multicast and unicast for MOH streaming. The advantage of using multicast for MOH streaming over unicast is to save bandwidth and to reduce the load on the MOH server. Saving bandwidth should not be a major issue for campus LAN environments, but reducing load on the MOH server, by reducing the number of media streams, is advantageous, especially when the MOH server is co-located on the same server with the Cisco CallManager service.

MOH Sources

MOH audio files are generated automatically by Cisco Unified Communications Manager when *.wav audio files are uploaded to the MOH server.

Music on Hold Sources

- MOH sources
 - One fixed source using a Cisco MOH USB audio sound card
 - 50 audio file sources
 - MOH Audio File Management converts the audio file
- Codecs used for MOH are G.711, G.729, and wideband
 - G.729 is developed and optimized for speech compression and reduces the music quality
- Consider the legalities and the ramifications of rebroadcasting copyrighted audio materials



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-35

MOH audio files are generated automatically by Cisco Unified Communications Manager when *.wav audio files are uploaded to the MOH server.

When the administrator imports an audio source file, the Cisco Unified Communications Manager Administration window interface processes the file and converts the file to the proper formats for use by the MOH server. The recommended format for audio source files includes the following specifications:

- 16-bit pulse code modulation (PCM) .wav file
- Stereo or mono
- Sample rates of 48 kHz, 32 kHz, 16 kHz, or 8 kHz

If recorded or live audio is needed, MOH can be generated from a fixed source. For this type of MOH, a sound card is required. The fixed audio source is connected to the audio input of the local sound card.

This mechanism enables the use of radios, CD players, or any other compatible sound source. The stream from the fixed audio source is transcoded in real time to support the codec that was configured through Cisco Unified Communications Manager Administration. The fixed audio source can be transcoded into G.711 (a-law or mu-law), G.729 Annex A, and wideband, and it is the only audio source that is transcoded in real time.

The Cisco MOH USB audio sound card (MOH-USB-AUDIO=) must be used for connecting a fixed or live audio source to the MOH server. This USB sound card is compatible with all MCS platforms supporting Cisco Unified Communications Manager Release 6.x.

Prior to using a fixed audio source to transmit MOH, consider the legalities and the ramifications of rebroadcasting copyrighted audio materials. Consult the legal department for potential issues.

Unicast MOH

Unicast MOH consists of streams sent directly from the MOH server to the endpoint requesting an MOH audio stream.

Unicast Music on Hold

Music on Hold unicast characteristics:

- Stream sent directly from MOH server to requesting endpoint
- Point-to-point, one-way audio stream
- Separate audio stream for each connection
- Negative effect on network throughput and bandwidth
- Unicast is useful in networks where multicast is not enabled and devices are not capable of multicast

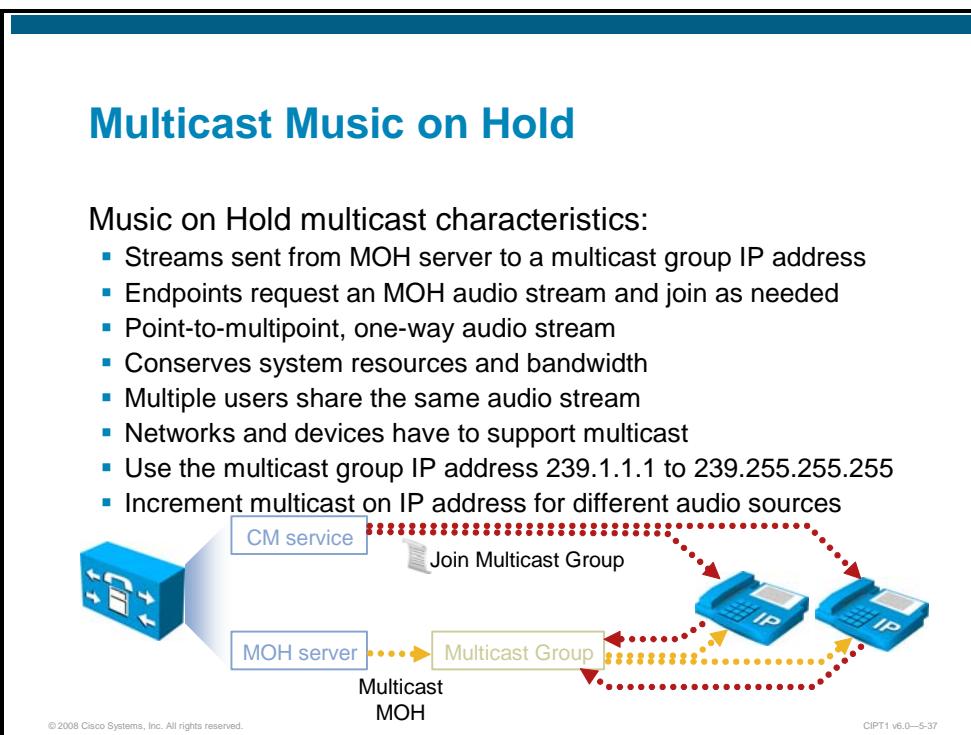
```
graph TD; CM[CM service] --> IP[IP Address]; IP --> MOH[MOH server]; MOH -.-> IP1[IP phone]; MOH -.-> IP2[IP phone]
```

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-36

A unicast MOH stream is a point-to-point, one-way audio RTP stream between the server and the endpoint device. Unicast MOH uses a separate source stream for each user or connection. As more endpoint devices go on hold via a user or network event, the number of MOH streams increases. Thus, if 20 devices are on hold, 20 streams of RTP traffic are generated over the network between the server and these endpoint devices. These additional MOH streams can potentially have a negative effect on network throughput and bandwidth. However, unicast MOH can be extremely useful in networks in which multicast is not enabled or devices are not capable of multicast, thereby still allowing an administrator to take advantage of the MOH feature.

Multicast MOH

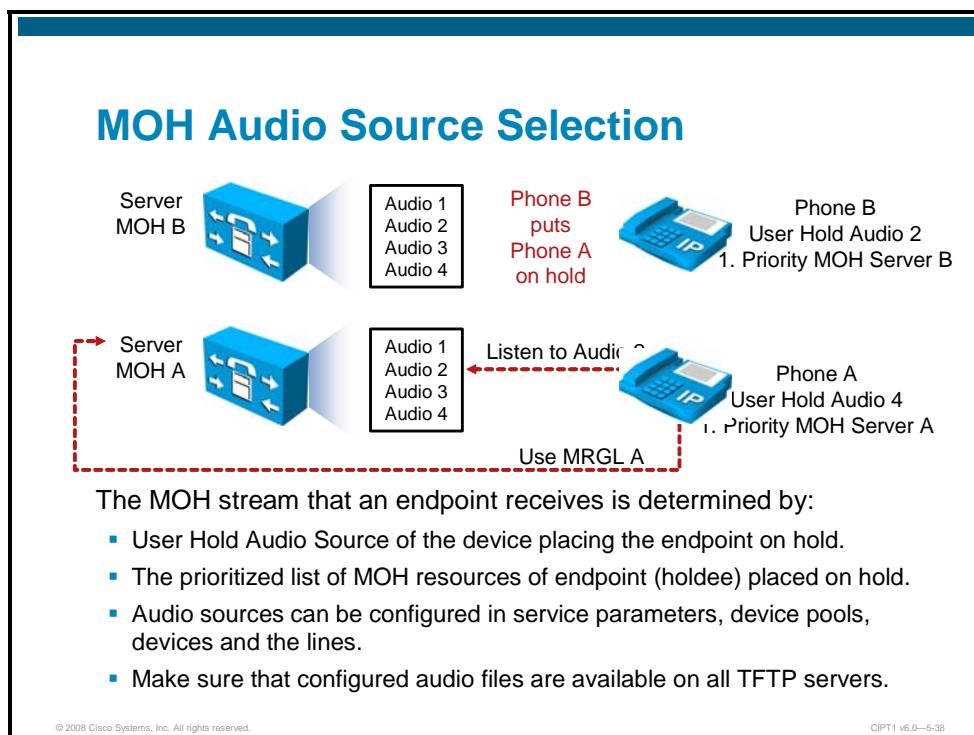
Multicast MOH consists of streams sent from the MOH server to a multicast group IP address, which endpoints requesting an MOH audio stream can join as needed.



A multicast MOH stream is a point-to-multipoint, one-way audio RTP stream between the MOH server and the multicast group IP address. Multicast MOH conserves system resources and bandwidth because it enables multiple users to use the same audio source stream to provide MOH. Thus, if 20 devices are on hold, potentially only a single stream of RTP traffic is generated over the network. For this reason, multicast is an extremely attractive technology for the deployment of a service such as MOH because it greatly reduces the CPU impact on the source device and also greatly reduces the bandwidth consumption for delivery over common paths. However, multicast MOH can be problematic in situations in which a network is not enabled for multicast or the endpoint devices are not capable of handling multicast.

MOH Audio Source Selection

This figure describes how the MOH audio source file and MOH audio server are selected in Cisco Unified Communications Manager.



The basic operation of MOH in a Cisco Unified Communications environment consists of a holder and a holdee. The holder is the endpoint user or network application placing a call on hold and the holdee is the endpoint user or device placed on hold.

The MOH stream that an endpoint receives is determined by a combination of the User Hold MOH Audio Source of the device placing the endpoint on hold (holder) and the configured prioritized list of MOH resources (Media Resource Group List [MRGL]) of the endpoint placed on hold (holdee). The User Hold MOH Audio Source configured for the holder determines the audio file that will be streamed when the holder puts a call on hold, and the prioritized list of MOH resources of the holdee is relevant to determine the server from which the holdee will receive the MOH stream.

The configuration of the holder determines which audio file to play and the configuration of the holdee determines which resource or server will play that file. In the figure, if phones A and B are on a call and phone B (holder) places phone A (holdee) on hold, phone A will hear the MOH audio source configured for phone B (Audio 2). However, phone A will receive this MOH audio stream from the resource or server configured for phone A.

Note When there is more than one MOH server active in your network, make sure that all the configured MOH files are available for all MOH servers. This may mean that the files must be copied manually to the root directories of all of the TFTP servers.

MOH Configuration

This topic describes the configuration of the Cisco Unified Communications Manager MOH feature.

Music on Hold Configuration Steps

1. Plan Music on Hold servers capacity
2. Configure Music on Hold audio sources
3. Check Music on Hold server configuration
4. Check Music on Hold service parameters
5. Optional: Configure multicast for Music on Hold
 - a) Configure MOH audio sources for multicast MOH
 - b) Configure MOH server for multicast MOH

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-40

Configuration of MOH consists of four main steps. Additional configuration is required if multicast MOH is used.

Step 1: Capacity Planning

The table in the figure lists the server platforms and the maximum number of simultaneous MOH sessions that each platform can support.

Step 1: Capacity Planning

Cisco Platform	Codecs	MOH Session
MCS 7815 MCS 7825	 G.711a, G711u G.729 Wideband	Co-resident or Standalone 250 MOH Streams
MCS 7835 MCS 7845	 G.711a, G711u G.729 Wideband	Co-resident or Standalone 500 MOH Streams

- The maximum of 51 unique audio sources counts for the cluster.
- 250 is the default value for unicast MOH sessions per server.
- Each multicast MOH audio source must be counted as two MOH streams.
- Maximum of 204 multicast streams (51 sources x 4 codec types).

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-41

As with all media resources, capacity planning is crucial to make certain that the hardware, once deployed and configured, can support the anticipated call volume of the network. For this reason, it is important to be aware of the hardware capacity for MOH resources and to consider the implications of multicast and unicast MOH in relation to this capacity. Ensure that network call volumes do not exceed these limits because, once MOH sessions have reached these limits, additional load could result in poor MOH quality, erratic MOH operation, or even loss of MOH functionality. The following MOH Server Configuration parameters affect MOH server capacity:

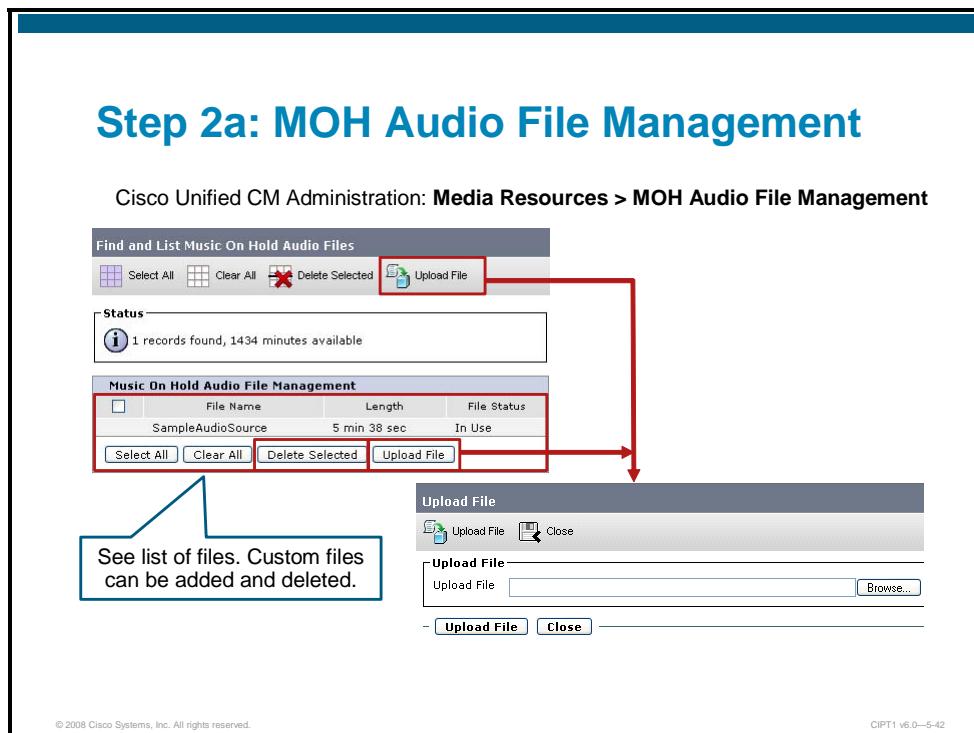
- **Maximum Half Duplex Streams:** This parameter determines the number of devices that can be placed on unicast MOH. By default, this value is set to 250. The Maximum Half Duplex Streams parameter should be set to the value derived from the following formula: (Server and deployment capacity) – ([Number of multicast MOH sources] x [Number of MOH codecs enabled]). The value of this parameter should never be set higher than the capacities indicated in the table based on the platform and deployment type (co-resident or standalone).
- **Maximum Multicast Connections:** This parameter determines the number of devices that can be placed on multicast MOH. By default, this value is set to 30,000. The Maximum Multicast Connections parameter should be set to a number that ensures that all devices can be placed on multicast MOH if necessary. Although the MOH server can generate only a finite number of multicast streams (maximum of 204), a large number of held devices can join each multicast stream. This parameter should be set to a number that is greater than or equal to the number of devices that might be placed on multicast MOH at any given time.

Typically, multicast traffic is accounted for based on the number of streams being generated; however, Cisco Unified Communications Manager maintains a count of the actual number of devices placed on multicast MOH or joined to each multicast MOH stream. This method is different than the way multicast traffic is normally tracked.

Note	Regarding the maximum recommended number of MOH streams (250 on Cisco MCS 7815 and 7825, and 500 on Cisco MCS 7835 and 7845) each multicast audio source has to be counted as two MOH streams. For example, if 3 multicast MOH audio sources and 4 codecs are enabled, no more than 476 unicast MOH streams should be generated at the same time ($2 \times 3 \times 4 + 476 = 500$).
-------------	---

Step 2a: MOH Audio File Management

The figure shows how to manage MOH audio files.



Cisco Unified Communications Manager, by default, has one MOH audio file, the Sample AudioSource. To add additional MOH audio files, go to **Media Resources > MOH Audio File Management** in Cisco Unified Communications Manager Administration and click **Upload File**.

The uploaded file is automatically converted into different audio formats (one per codec). At the Find and List Music On Hold Audio Files window, which is accessed via **Media Resources > MOH Audio File Management**, a file status of Translation Complete indicates that the audio file has been successfully converted. For audio files that have already been successfully converted and are already configured as an MOH audio source, the file status is In Use. During the conversion, the status is Open.

If any other status is displayed, or if the status remains Open for a longer period of time, the audio file translation fails. Depending on the size of the audio file and the load on the server, conversion can take up to several minutes. The uploaded audio file must be in .wav file format. The file must meet the following specifications:

- 16-bit PCM .wav file
- Stereo or mono
- Sample rates of 48 kHz, 32 kHz, 16 kHz, or 8 kHz

Delete the files that were not able to be translated from **Media Resources > MOH Audio File Management**.

Note	The upload of MOH files must be performed separately at each MOH server. In order to upload the files to an MOH server, use the IP address of the MOH server (rather than the publisher IP address) in the Cisco Unified Communications Manager Administration URL (<a href="https://<IP address of MOH server>/ccmadmin">https://<IP address of MOH server>/ccmadmin) before selecting Media Resources > MOH audio file management .
-------------	---

Step 2b: MOH Audio Sources Configuration: MOH Audio Source

The figure shows how to configure MOH audio sources, which can then be selected at devices, lines, or device pools.

Step 2b: MOH Audio Sources Configuration: MOH Audio Source

Cisco Unified CM Administration: **Media Resources > Music On Hold Audio Source**

Music On Hold Audio Source Configuration

Save Delete Add New Upload File

Music On Hold Server Audio Source Information

MOH Audio Stream Number*	2
MOH Audio Source File	carry on
MOH Audio Source Name*	carry on
<input checked="" type="checkbox"/> Play continuously (repeat)	
<input type="checkbox"/> Allow Multicasting	

MOH Audio Source File Status

InputFileName: carry on
ErrorCode: 0
ErrorText: Translation Complete
DurationSeconds: 4
DiskSpaceKB: 196
LastUpdate: 1190803264
HighDefTime: 0
OutputFileList:
carry on.ulaw.wav
carry on.alaw.wav
carry on.g729.wav

Select audio source number 1-51.

Select audio source file for selected audio source number.

Enter audio source name.

Enable or disable audio file repeat.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-43

To configure MOH audio sources, in Cisco Unified Communications Manager Administration, go to **Media Resources > Music On Hold Audio Source**. The MOH audio sources are identified by an MOH Audio Stream Number (1–51).

In the Music On Hold Audio Source Configuration window, first, select the MOH Audio Stream Number of the audio source that you want to configure. Then choose the MOH Audio Source File. The MOH Audio Source Name defaults to the MOH Audio Source File name and can be modified. Finally enable or disable continuous playing (repeat) of the audio file.

Step 2b: MOH Audio Sources Configuration: Fixed MOH Audio Source

A fixed MOH audio source can be configured in order to allow audio from an external device to be played instead of playing MOH from locally stored MOH files.

Step 2b: MOH Audio Sources Configuration: Fixed MOH Audio Source

Cisco Unified CM Administration: **Media Resources > Fixed MOH Audio Source**

Fixed MOH Audio Source Configuration

Save Delete

Status —

Status: Ready

Fixed MOH Audio Source Information —

Source ID * **51**

Name *

Allow Multicasting

Enable (if checked, Name is required.)

Enter the name of the fixed MOH audio source

Enable the fixed MOH audio source

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-44

To configure a fixed MOH audio source, in Cisco Unified Communications Manager Administration, go to **Media Resources > Fixed MOH Audio Source**. The Source ID is 51 and cannot be modified (only one fixed MOH audio source can be configured in a Cisco Unified Communications Manager cluster). You must enter the name and enable the fixed MOH audio source.

Step 3: MOH Server Configuration

The Cisco Unified Communications Manager MOH server is automatically added when the Cisco IP Voice Media Streaming App services are activated.

Step 3: MOH Server Configuration

Cisco Unified CM Administration: Media Resources > Music On Hold Server

Music On Hold (MOH) Server Configuration

Device Information

Registration	Registered with Cisco Unified Communications Manager 10.1.1.1
IP Address*	10.1.1.1
Host Server*	10.1.1.1
Music On Hold Server Name*	MOH_2
Description	MOH_CUCM1-1
Device Pool*	Default
Location*	Hub_None
Maximum Half Duplex Streams*	250
Maximum Multicast Connections*	30
Fixed Audio Source Device	
Run Flag*	Yes

Multicast Audio Source Information

The MOH server is automatically added with default values when the IP Voice Media Streaming App services are activated.

© 2008 Cisco Systems, Inc. All rights reserved.CIPT1 v6.0—5-45

The figure shows the default configuration of the MOH media resource. You can modify parameters such as Name, Description, Device Pool, Location, and Maximum Half Duplex Streams (that is, unicast MOH streams).

If a fixed audio source that is physically connected to the server is used, the name of the audio source device must be specified.

Step 4: MOH Service Parameters

The figure lists the relevant service parameters for MOH.

Step 4: MOH Service Parameters

- IP Voice Media Streaming Application service
 - Supported MOH codecs (G.711, G729a, wideband)
 - QoS for MOH (signaling and audio)
 - Packet size for G.711, G.729, and wideband (20 ms)
- CallManager service
 - Suppress MOH to Conference Bridge (True)
 - Default Network Hold MOH Audio Source ID (1)
 - Default User Hold MOH Audio Source ID (1)
 - Duplex Streaming Enabled (False)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-46

The default parameters are shown in parenthesis. These service parameters only need to be configured if there is a need to use nondefault values.

Note	These service parameters can be accessed from System > Service Parameters . Note that some of them are Cisco IP Voice Media Streaming Application service parameters and others are Cisco CallManager service parameters.
-------------	---

Step 5a: Multicast MOH – Audio Sources Configuration

In order to enable multicast MOH, multicast MOH first has to be allowed on MOH audio sources, as shown in the figure.

Step 5a: Multicast MOH – Audio Sources Configuration

Music On Hold Audio Source Configuration

Music On Hold Server Audio Source Information

MOH Audio Stream Number*

MOH Audio Source File

MOH Audio Source Name*

Play continuously (repeat)

Allow Multicasting

MOH Audio Source File Status

InputFileName: Sample AudioSource
ErrorCode: 0
ErrorText: Translation Complete
DurationSeconds: 338
DiskSpaceKB: 8092
LowDateTime: 1130860118
HighDateTime: 0
OutputFileList:

Fixed MOH Audio Source Configuration

Status

i Status: Ready

Fixed MOH Audio Source Information

Source ID*

Name*

Allow Multicasting

Enable (If checked, MOH audio source is required.)

In order to use multicast MOH, multicast MOH has to be enabled at MOH audio sources.

MOH audio sources are not configured for multicast MOH use by default.
MOH audio sources and fixed MOH audio sources (if used) need to be enabled for multicast MOH.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-47

Click the Allow Multicasting check box for each MOH audio source that is allowed to be sent as a multicast stream. This applies to MOH audio sources and to fixed MOH audio sources.

Step 5b: Multicast MOH – MOH Server Configuration

After allowing multicast MOH on audio sources, the MOH server must be enabled for multicast MOH, as shown in the figure.

Step 5b: Multicast MOH – MOH Server Configuration

Cisco Unified CM Administration: **Media Resources > Music On Hold Server**

Music On Hold (MOH) Server Configuration

Multicast Audio Source Information

Enable Multicast Audio Sources on this MOH Server
Base Multicast IP Address*: 239.1.1.1
Base Multicast Port Number*: 16384 (Even numbers only)
Increment Multicast on*: Port Number IP Address

Selected Multicast Audio Sources

No.	Audio Source Name	Max Hops
1	Sample AudioSource	2

Enable multicast MOH on the MOH server

Configure multicast parameters

Set maximum hops (Time To Live) value per audio source for multicast packets

In order to use multicast MOH, multicast MOH has to be enabled at the Music On Hold Server configuration window.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-48

The figure shows how to enable multicast MOH on an MOH server. In the Multicast Audio Source Information section of the MOH Server configuration window, click the Enable Multicast Audio Sources on this MOH Server check box. The Base Multicast IP Address, Base Multicast Port Number, and Increment Multicast On parameters are automatically populated after you enable multicast MOH on the server. You can modify these values as desired.

Note It is recommended to increment multicast on IP address instead of port number to avoid network saturation in firewall situations. This results in each multicast audio source having a unique IP address and helps to avoid network saturation.

All MOH audio sources that have been configured to allow multicasting are listed in the Selected Multicast Audio Sources section of the MOH Server configuration window. You can set the Max Hops value for each audio source (default is 2). This parameter sets the Time to Live (TTL) value in the IP header of the multicast MOH RTP packets to the specified value. TTL in an IP packet indicates the maximum number of routers that an audio source is allowed to cross. If Max Hops is set to zero, the multicast MOH RTP packets remain in the subnet of the multicast MOH server. If Max Hops is set to 1, the audio source can cross up to one router to the next subnet. Cisco recommends setting max hops to 2.

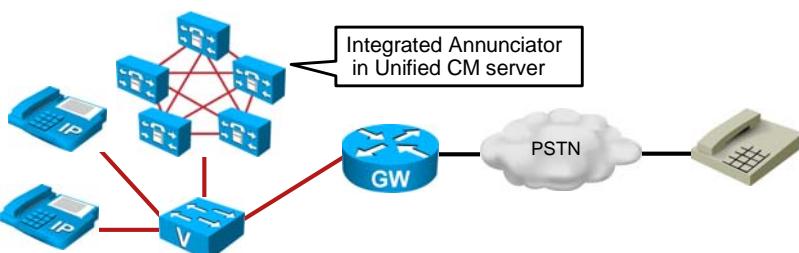
Note When using multicast MOH, and when the devices that should listen to multicast MOH streams are not in the same IP network, multicast routing has to be enabled in the IP network. Take care when enabling multicast routing in order to avoid parts of the network being flooded with mis-sent multicast packets (especially across WAN links). This can be achieved by disabling multicasts on interfaces on which the multicast MOH packets are not required, and by the Max Hops parameter discussed earlier.

Note	When media resource groups and media resource group lists are used to implement media resources access control, and a multicast MOH server is assigned to a media resource group, multicast MOH also has to be enabled at the media resource group in order to use multicast MOH.
-------------	---

Annunciator Essentials

This topic describes the function and features of the Cisco Unified Communications Managers integrated annunciator.

Annunciator Overview



- The annunciator is part of the Cisco IP Voice Media Streaming Application service.
- Annunciator streams spoken messages and various call progress tones.
- Receiving devices such as IP phones or gateways must be capable of SCCP to utilize this feature.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-50

An annunciator is automatically created in the system when the Cisco IP Voice Media Streaming Application is activated on a server. If the Cisco IP Voice Media Streaming Application is deactivated, the annunciator is deleted. A single annunciator instance can service the entire Cisco Unified Communications Manager cluster if it meets the performance requirements; otherwise, you must configure additional annunciators for the cluster. Additional annunciators can be added by activating the Cisco IP Voice Media Streaming Application on other servers within the cluster.

The annunciator registers with a single Cisco Unified Communications Manager at a time, as defined by its device pool. It will automatically fail over to a secondary Cisco Unified Communications Manager if a secondary is configured for the device pool. Any announcement that is playing at the time of an outage will not be maintained.

An annunciator is considered a media device, and it can be included in a Media Resource Group (MRG), which can control which annunciator is selected for use by phones and gateways.

Annunciator Features and Capacities

This subtopic describes annunciator features and capacities.

Annunciator Features and Capacities

- Tones and announcements are predefined.
- The announcements support localization and may be customized by replacing the appropriate .wav file.
- The annunciator is capable of supporting G.711, G.729, and wideband codecs without any transcoding resources.
- The following features require an annunciator:
 - Cisco Multilevel Precedence Preemption (call failure)
 - Integration via SIP trunk (call progress and DTMF tones)
 - Cisco IOS gateways and intercluster trunks (ringback)
 - System messages (call failure)
 - Conferencing (Barge tone)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-51

The following features require an annunciator resource:

- **Cisco Multilevel Precedence and Preemption (MLPP):** This feature has streaming messages that it plays in response to the following call failure conditions:
 - Unable to preempt due to an existing higher-precedence call.
 - A precedence access limitation was reached.
 - The attempted precedence level was unauthorized.
 - The called number is not equipped for preemption or call waiting.
- **Integration via SIP trunk:** SIP endpoints have the ability to generate and send tones in-band in the RTP stream. Because SCCP devices do not have this ability, an annunciator is used in conjunction with an MTP to generate or accept dual tone multifrequency (DTMF) tones when integrating with a SIP endpoint. The following types of tones are supported:
 - Call progress tones (busy, alerting, and ringback)
 - DTMF tones
- **Cisco IOS gateways and intercluster trunks:** These devices require support for call progress tone (ringback tone).
- **System messages:** During the following call failure conditions, the system plays a streaming message to the end user:
 - A dialed number that the system cannot recognize
 - A call that is not routed due to a service disruption
 - A number that is busy and not configured for preemption or call waiting

- **Conferencing:** During a conference call, the system plays a barge-in tone to announce that a participant has joined or left the bridge.

Annunciator Performance

By default, the annunciator is configured to support 48 simultaneous streams, which is the maximum recommended for an annunciator running on the same server (co-resident) with the Cisco Unified Communications Manager service.

Annunciator Performance

- A standalone server without the Cisco CallManager service can support up to 255 simultaneous announcement streams.
- High-performance server with dual CPUs can support up to 400 announcement streams.
- Default is 48 announcement streams and recommended when co-resident.
- Multiple standalone servers can be integrated to support the required number of announcement streams.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-52

If the server has only 10-Mbps connectivity, lower the setting to 24 simultaneous streams. A standalone server without the Cisco CallManager service can support up to 255 simultaneous announcement streams, and a high-performance server with dual CPUs and a high-performance disk system can support up to 400 streams. Multiple standalone servers can be added to support the required number of streams.

Annunciator Configuration

The annunciator media resource is automatically added when the Cisco IP Voice Media Streaming Application service is activated.

Annunciator Media Resource Configuration Steps

Cisco Unified CM Administration: **Media Resources > Annunciator**

Annunciator Configuration Related Links: [Back To Find>List](#) [Go](#)

[Save](#) [Reset](#)

Status
Status: Ready

Modify default values if desired.

Device Information

Registration	Registered with Cisco Unified Communications Manager 10.1.1.1
IP Address	10.1.1.1
Server*	10.1.1.1
Name*	ANN_2
Description	ANN_CUCM1-1
Device Pool*	Default
Location*	Hub_None

- [Save](#) [Reset](#) -

The annunciator is automatically added with default values when the IP Voice Media Streaming App services are activated.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-53

The figure shows the default configuration of the annunciator. The only configurable items are Name, Description, Device Pool, and Location.

Media Resources Access Control Essentials

This topic describes a way to restrict access to Cisco Unified Communications Manager media resources.

The Need for Media Resource Access Control

- By default, all existing media resources usage is load-balanced.
- Usage of the hardware conference resources is preferred.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-55

The figure shows a phone in need of selecting a conference media resource.

By default, all existing media resources are located in a “Null” Media Resource Group and usage of them is load-balanced between all existing devices. Usage of the hardware conference resources is preferred because of their enhanced capabilities (mixed-mode conferences) and the reduction of load on the Cisco Unified Communications Manager integrated software conference bridges.

Media Resource Management controls and manages the media resources within a cluster, allowing all Cisco Unified Communications Manager servers within the cluster to share media resources.

Media Resource Management enhances Cisco Unified Communications Manager features by making it easier for Cisco Unified Communications Manager to deploy transcoder, annunciator, conferencing, MTP, and MOH resources. Media Resource Management distribution throughout the Cisco Unified Communications Manager cluster uses these resources to their full potential, which makes the Cisco Unified Communications Manager cluster efficient and economical.

Media Resource Access Control

This subtopic describes some of the reasons to use media resource access control:

Media Resources Access Control

- Enables hardware and software devices to coexist within a Unified CM and to be used with different priorities.
- Shares and accesses the resources that are available in the cluster.
- Performs load distribution within a group of similar media resources.
- Allows media resource access control based on type of resource.
- Media resources are bundled in load-balanced Media Resource Groups (MRGs).
- Media Resource Groups are listed in prioritized Media Resource Group Lists (MRGLs).

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-56

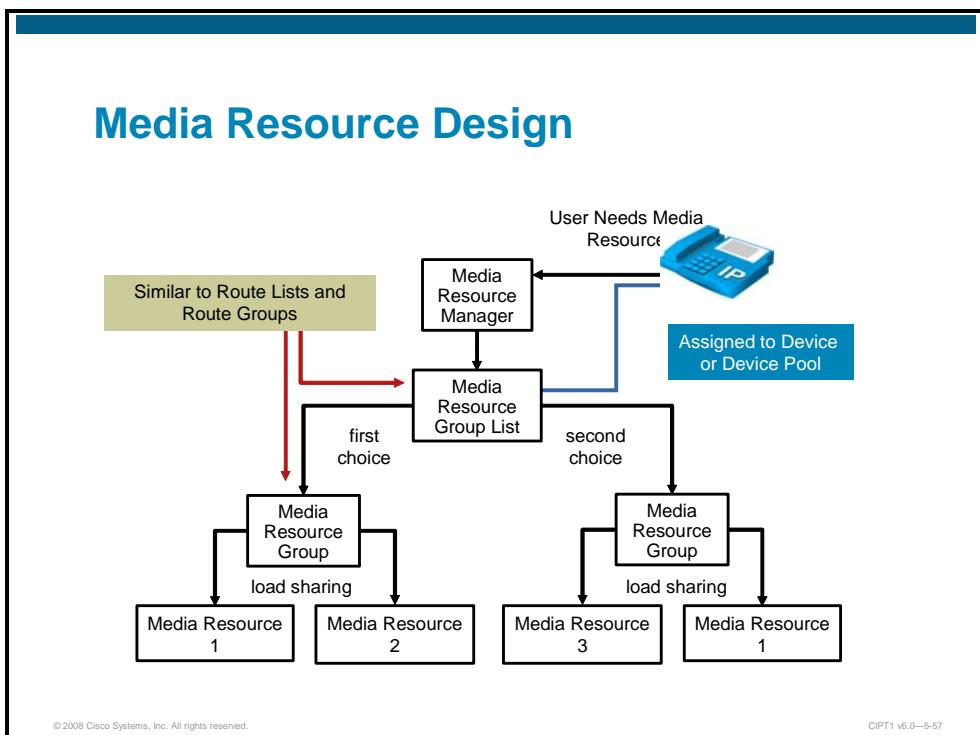
Some of the reasons to use media resources access control are as follows:

- To enable hardware and software media resources to coexist within a Cisco Unified Communications Manager and to be used with different priorities.
- To enable Cisco Unified Communications Manager to share and access the resources that are available in the cluster.
- To enable Cisco Unified Communications Manager to perform load distribution within a group of similar media resources.
- To allow media resource access control based on type of resource, such as, for example, if there is one user allowed to use a hardware conference bridge while another user is not allowed.

Media Access Control bundles media resources in load-balanced MRGs, which are listed in prioritized MRGLs.

Media Resource Design

Cisco Unified Communications Manager MRGs and MRGLs provide a way to manage resources within a cluster.



MRGs define logical groupings of media servers. Associate an MRG with a geographical location or a site as desired. Form MRGs to control the usage of servers or the type of service (unicast or multicast) that is desired.

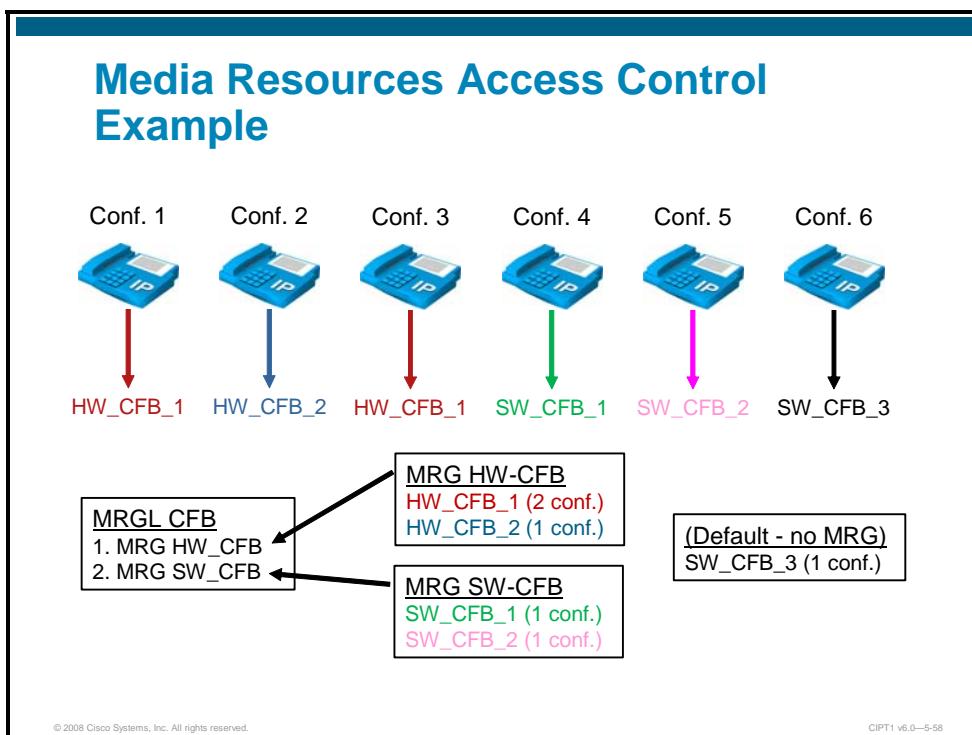
MRGLs specify a list of prioritized MRGs. An application can select required media resources from among the available resources according to the priority order that is defined in the MRGL. MRGLs, which are associated with devices, provide MRG redundancy.

The figure shows the hierarchical ordering of media resources and how MRGs and MRGLs are similar to route groups and route lists.

Note	When a device needs a media resource, it searches its own MRGL first. If a media resource is not available, the device searches the default list, which includes all of the media resources that have not been assigned to an MRG. After a resource is assigned to an MRG, it is removed from the default list.
-------------	---

Media Resource Access Control Example

The figure shows how media resources are allocated to devices when they are listed in MRGs and MRGLs.



In the example, there are five conference bridges:

- HW_CFB_1: For the example we assume that it has capacity for 2 conferences.
- HW_CFB_2: For the example we assume that it has capacity for 1 conference.
- SW_CFB_1: For the example we assume that it has capacity for 1 conference.
- SW_CFB_2: For the example we assume that it has capacity for 1 conference.
- SW_CFB_3: For the example we assume that it has capacity for 1 conference.

HW_CFB_1 and HW_CFB_2 are in MRG_HW-CFB, SW_CFB_1 and SW_CFB_2 are in MRG_SW-CFB and SW_CFB_3 is not assigned to an MRG.

MRGL_MRGL_CFB has MRG_MRGL_CFB listed before MRG_MRGL_SW-CFB.

If you assume that six conferences are established from devices which all use the MRGL_MRGL_CFB, the conference bridges will be allocated in the following way:

The first conference uses conference bridge HW_CFB_1. The second conference uses conference bridge HW_CFB_2 because the resources within an MRG are load-shared and not used in the configured order. Due to the load-sharing algorithm, the third conference uses HW_CFB_1 again.

Because no resource is left in the first MRG of the MRGL, the fourth conference uses a resource of the second MRG: conference bridge SW_CFB_1. The fifth conference uses SW_CFB_2.

The sixth conference does not find a free resource in any MRG of the MRGL and finds a conference resource in the default list (that is, the list of resources that have not been assigned to any MRG): SW_CFB_3.

Media Resource Access Control Configuration

This topic describes how to configure media resource access control.

Media Resource Group List Configuration Steps

1. Configure Media Resource Groups
2. Configure Media Resource Group Lists
3. Assign the Media Resource Group Lists to phones

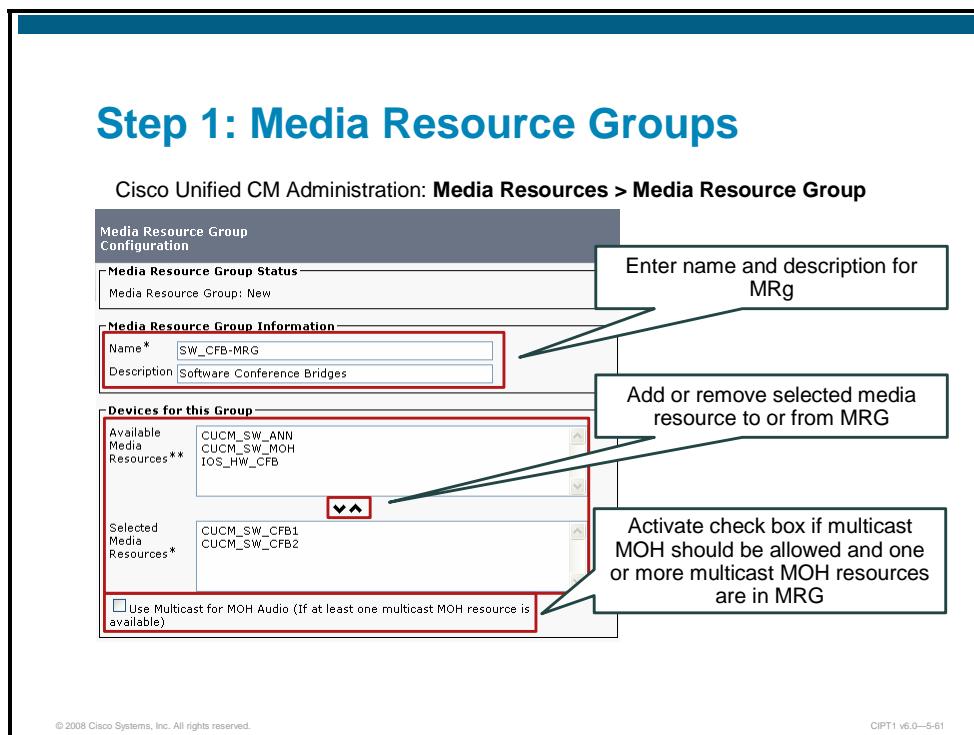
© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-60

The figure shows the three configuration steps that are required to configure media resource access control.

Step 1: Configure MRGs

The figure shows the configuration of a Media Resource Group.

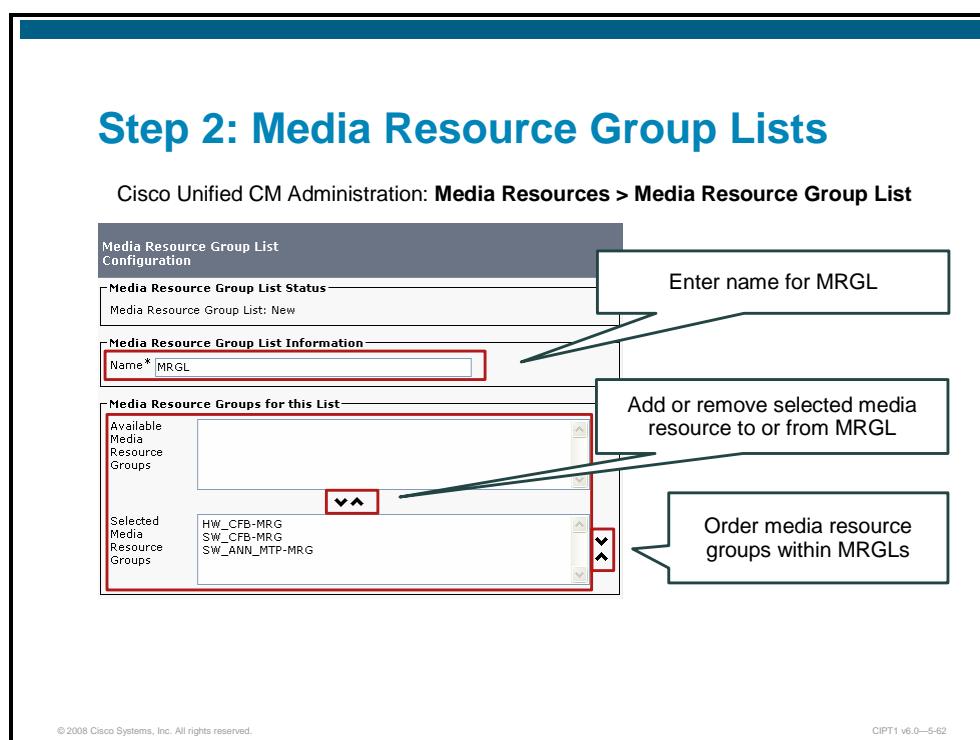


To add an MRG, go to **Media Resources > Media Resource Group** in Cisco Unified Communications Manager Administration. In the Media Resource Group Configuration window, enter a name and description for the MRG and add the desired media resources to the MRG.

Note If the MRG includes one or more multicast MOH servers and multicast MOH should be allowed by this MRG, click the **Use Multicast for MOH Audio** check box.

Step 2: Configure MRGLs

The figure shows the configuration of an MRGL.



To add an MRGL, go to **Media Resources > Media Resource Group List** in Cisco Unified Communications Manager Administration. At the Media Resource Group List Configuration window, enter a name for the MRGL and add the desired media resource groups to the MRGL.

As the order of MRGs within a MRGL specifies the priorities of the MRGs, it is important to list the media resource groups in the desired order. In the example, hardware conference bridges should be used before software conference bridges.

Note	The order of MRGs is only relevant if multiple MRGs with the same type of media resources exist. In the example, only one MRG includes annunciators and MTPs (SW_ANN_MTP-MRG). If Cisco Unified Communications Manager searches for an MTP, the first two MRGs are ignored because they do not include an MTP resource. If a conference resource has to be allocated, the two MRGs that include conference bridges are searched in order.
-------------	---

Step 3: Configure Phones with MRGLs

The figure shows how to assign an MRGL to an IP phone.

Step 3: Configure Phones with Media Resource Group Lists

Cisco Unified CM Administration: **Device > Phone**

Phone Configuration

Phone Type

Product Type: Cisco 7961
Device Protocol: SIP

Device Information

Registration	Registered with Cisco Unified Communications Manager 10.1.1.1
IP Address	10.1.1.21
MAC Address*	00070E576F43
Description	Phone2
Device Pool*	Default
Common Device Configuration	< None >
Phone Button Template*	Standard 7961 SIP
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	MRGL-HQ
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >

Assign MRGL to IP phone

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-63

MRGLs can be assigned to devices (such as phones, trunks or gateways) or to device pools. In the example, the previously configured MRGL, MRGL-HQ, is assigned to an IP phone.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Media Voice Termination required for Voice Termination, audio conferencing, transcoding, Media Termination Point, annunciator, Music on Hold.
- There are no direct endpoint-to-endpoint audio streams if a media resources is involved.
- Only some hardware-based conference bridges support mixed-mode conferences with participants using different codecs.
- It is possible to configure external conference bridges to enhance the conferencing capabilities of the Unified CM.
- If the IP Voice Media Streaming Application service is running, conferencing hardly needs additional configuration steps.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-64

Summary (Cont.)

- The maximum of 51 unique audio sources counts for the cluster. For a fixed audio source, a Cisco MOH USB audio sound card is required.
- The MOH stream that an endpoint receives is determined by the User Hold Audio Source of the device placing the endpoint on hold and the configured MRGL of the endpoint being placed on hold.
- The annunciator streams spoken messages and various call progress tones to devices supporting SCCP.
- The Media Resource Manager controls the media resources within a Cisco Unified Communications Manager cluster. The media resources are shared within a cluster.
- To limit media resources access, Media Resource Groups and Media Resource Group Lists have to be configured and assigned.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-65

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager Features and Services Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfeat/fsgd.pdf

Lesson 2

Configuring Cisco Unified Communications Manager User Features

Overview

This lesson describes Cisco Unified Communications Manager features such as Call Park, Directed Call Park, Do Not Disturb (DND), Hold Reversion, Intercom, Cisco Call Back, Barge, Privacy, and Call Pickup, and explains how to configure these features. It provides information about softkeys, phone button templates, user web pages, and Cisco IP Phone Services.

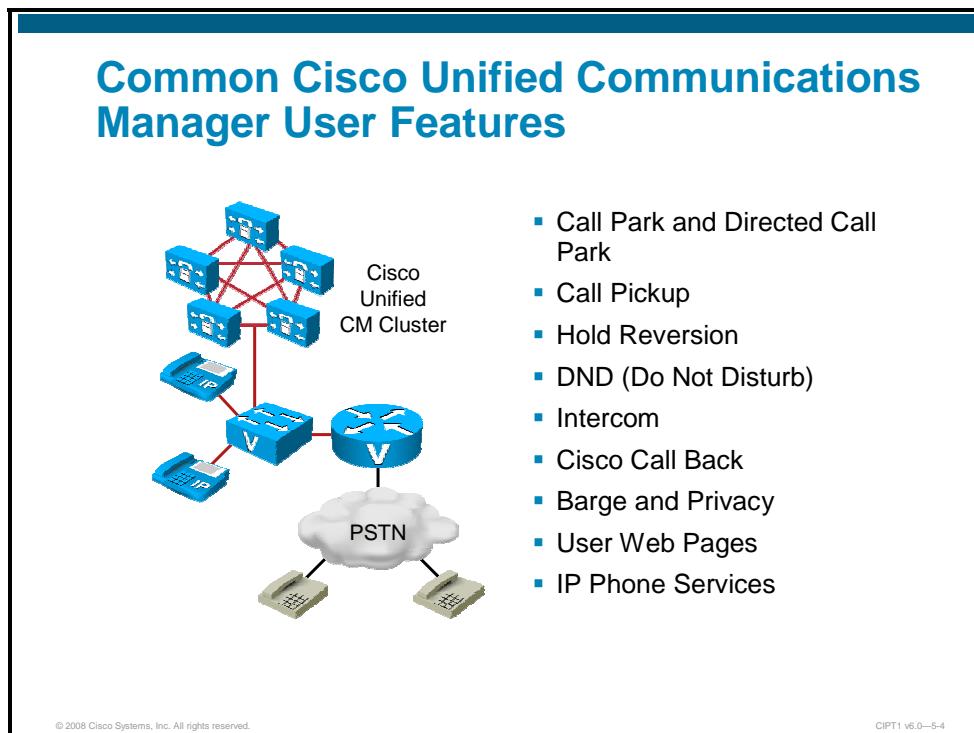
Objectives

Upon completing this lesson, you will be able to describe and configure Cisco Unified Communications Manager user features. This ability includes being able to meet these objectives:

- Explain Cisco Unified Communications Manager user features
- Describe Call Park and Directed Call Park
- Describe Call Pickup and Hold Reversion
- Describe DND, Intercom, and Cisco Call Back
- Describe Barge and Privacy
- Describe user web pages
- Describe Cisco IP Phone Services

Cisco Unified Communications Manager User Features

This topic describes Cisco Unified Communications Manager user features and provides an overview of the different services.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-4

Some common Cisco Unified Communications Manager user features are listed in the figure. The table gives a short description of these features.

Description of User Features

Feature Name	Description
Call Park	Allows you to place a call on hold, so it can be retrieved from another phone in the Cisco Unified Communications Manager system.
Directed Call Park	Allows you to transfer a call to an available user-selected Directed Call Park number.
Call Pickup	Allows you to pick up incoming calls.
Hold Reversion	Alerts a phone user when a held call exceeds a configured time limit.
DND	Allows turning off the ringer for an incoming call.
Intercom	A new type of phone line. It combines the functionality of a traditional line and a speed dial.
Cisco Call Back	Allows receiving call-back notification on your Cisco Unified IP phone when a called party line becomes available.
Barge and Privacy	Barge adds a user to a call that is in progress.
User Web Pages	Allows users to configure their IP phones from a web page.

Feature Name	Description
Cisco IP Phone Services	Cisco Unified IP Phone Services comprise XML applications that enable the display of interactive content with text and graphics on Cisco Unified IP phones.

Various other features are available with Cisco Unified Communications Manager but are not discussed in this course. These features are listed in the following table:

Further User Features

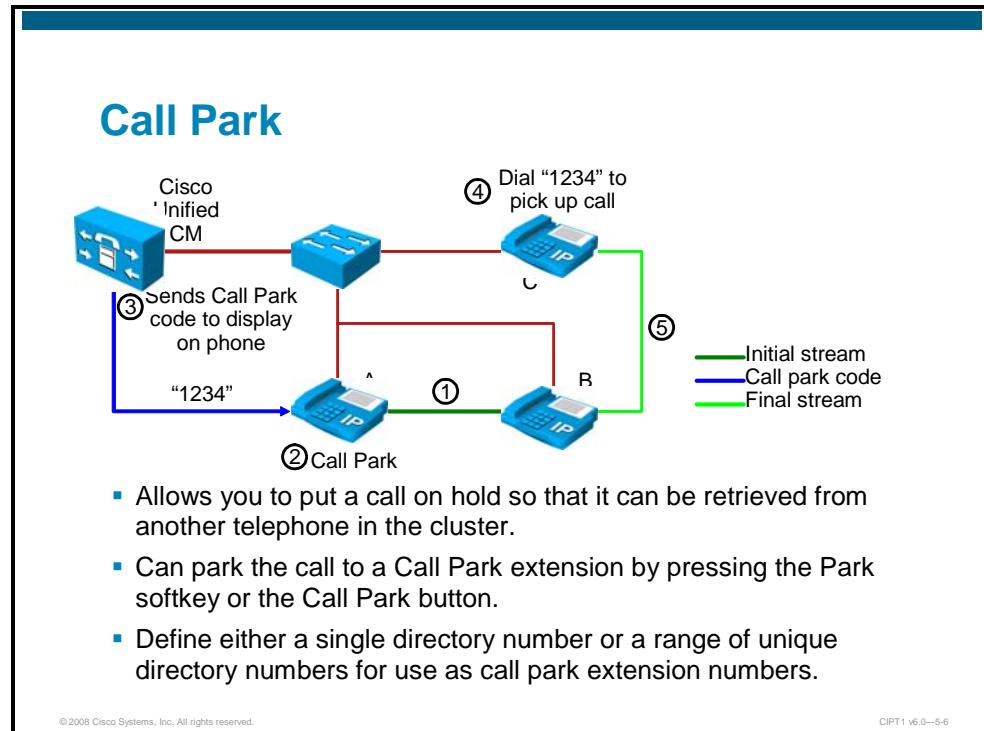
Feature Name	Description
Cisco Extension Mobility	Allows users to temporarily access their Cisco Unified IP phone configuration such as line appearances, services, and speed dials from other Cisco Unified IP phones.
Cisco Unified Communications Manager Assistant	Enables managers and their assistants to work together more effectively.
Client Matter Codes and Forced Authorization Codes	Forced Authorization Codes (FAC) and Client Matter Codes (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients, while FAC regulate the types of calls that certain users can place.
Music on Hold (MOH)	The integrated MOH feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source.
Cisco Unified Communications Manager Auto-Attendant	A simple automated attendant, allows callers to locate people in your organization without talking to a receptionist.
Immediate Divert (iDivert)	Allows you to immediately divert a call to a voice-messaging system.
Malicious Call Identification (MCID)	A supplementary service that allows you to report a call of a malicious nature by requesting that Cisco Unified Communications Manager identify and register the source of an incoming call in the network.
Multilevel Precedence and Preemption (MLPP)	A service allows properly validated users to place priority calls. If necessary, users can preempt lower priority phone calls.
Custom Phone Rings	Allows users to customize the phone ring types that are available at their sites.
Cisco Web Dialer	Allows Cisco Unified IP phone users to make calls from web and desktop applications.
Cisco Unified Communications Manager Attendant Console	A client-server application, allows you to use a graphical user interface that contains speed-dial buttons and quick directory access to look up phone numbers, monitor line status, and direct calls. A receptionist or administrative assistant can use the attendant console to handle calls for a department or company.
Call Display Restrictions	Allows you to choose the information that will display for calling or connected lines, depending on the parties who are involved in the call.
Quality Report Tool (QRT)	A voice-quality and general problem-reporting tool for Cisco Unified IP phones, which acts as a service to allow users to easily and accurately report audio and other general problems with their IP phones.
External Call Transfer Restrictions	Allows the Cisco Unified Communications Manager administrator to configure gateways, trunks, and route patterns as on-net (internal) or off-net (external) devices at the system level.

Feature Name	Description
Presence	Allows a user to monitor the real-time status of another user at a directory number or session initiation protocol (SIP) Uniform Resource Identifier (URI).
Cisco Unified Communications Manager Device Mobility	Dynamically changes important location settings, such as calling search space, region, date/time group, and Survivable Remote Site Telephony (SRST) reference, for roaming devices.
Mobile Connect and Mobile Voice Access	Mobile Connect enables users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. Mobile Voice Access extends Mobile Connect capabilities by way of an integrated voice response (IVR) system used to initiate Enterprise Mobile Connect Calls using a remote phone (such as a cell phone).
Monitoring and Recording	The Silent Call Monitoring feature allows a supervisor to eavesdrop on a conversation between a call center agent and a customer without allowing the agent to detect the monitoring session.

Note For more information regarding these and other Cisco Unified Communications Manager features, refer to *Cisco Unified Communications Manager Features and Services Guide*, Release 6.0(1), at
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfeat/fsgd.pdf.

Call Park and Directed Call Park

This topic describes Call Park and Directed Call Park, and discusses how to configure these features.



The Call Park feature allows you to put a call on hold so that it can be retrieved from another phone in the Cisco Unified Communications Manager cluster. (For example, a call can be “parked” in the office and retrieved in a conference room.)

If an active call is on the phone, the call can be parked to a Call Park extension by pressing the Park softkey or the **Call Park** button. By dialing the Call Park extension from another phone in the system, the call can be retrieved.

The Call Park feature works within a Cisco Unified Communications Manager cluster and, for this to function properly, each Cisco Unified Communications Manager in a cluster must have call park extension numbers defined. Either a single directory number or a range of directory numbers can be defined for use as call park extension numbers. Call park numbers cannot overlap between Cisco Unified Communications Manager servers. Ensure that each Cisco Unified Communications Manager server has its own number range.

Cisco Unified Communications Manager can park only one call at each call park extension number.

The figure illustrates how to use the Call Park feature, as follows:

1. User on phone A calls phone B.
2. User on phone A wants to take the call in a conference room for privacy. Phone A user presses the Park softkey.
3. The Cisco Unified Communications Manager server to which phone A is registered sends the first available call park directory, 1234, which displays on phone A. The user on phone A watches the display for the call park directory number (to dial that directory number on phone C).

4. The user on phone A leaves the office and walks to an available conference room where the phone is designated as phone C. The user goes off-hook on phone C and dials 1234 to retrieve the parked call.
5. The system establishes the call between phones C and B.

The Call Park feature can also be used across Cisco Unified Communications Manager clusters. Users can dial the assigned route pattern (for example, a route pattern for an intercluster trunk could be 80XX) and the Call Park number (for example, 8022) to retrieve parked calls from another Cisco Unified Communications Manager cluster. Ensure that Calling Search Spaces (CSSs) and partitions are properly configured.

Call Park Configuration

This subtopic describes how to configure Call Park.

Call Park Configuration

Call Park Configuration.

Call Park Number/Range*	166X
Description	Call Park DN
Partition	< None >
Cisco Unified CallManager*	CM_California

— Save —

▪ Ensure that Call Park number or range is unique within the cluster and that each Cisco Unified CM that devices are registered to has its own unique Call Park number or range.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-7

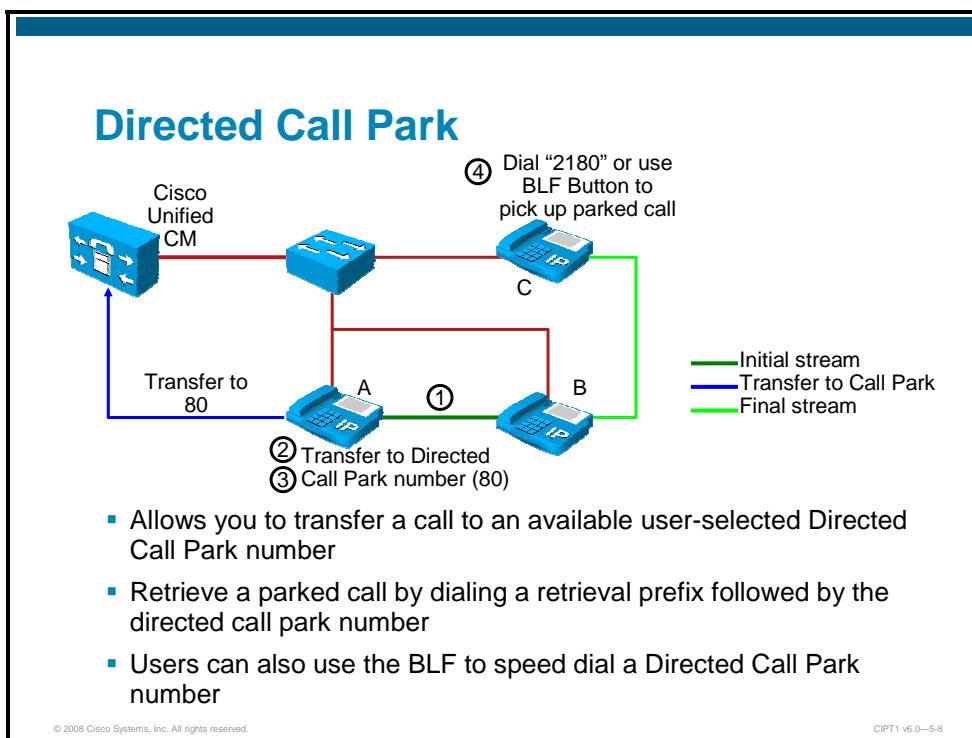
A Call Park number or range must be configured for each Cisco Unified Communications Manager in the cluster. When the Call Park feature is invoked, it is assigned a Call Park code. A user uses this code to pick up the call from another Cisco IP phone on the same Cisco Unified Communications Manager that the original IP phone is registered to. When the Call Park number or range is assigned to a partition, access to the Call Park feature can be limited based on the device CSS. Ensure that the Call Park number or range is unique throughout the Cisco Unified Communications Manager cluster.

You can access the Call Park feature in Cisco Unified Communications Manager Administration by choosing **Call Routing > Call Park**.

Valid call park extension numbers comprise integers and the wildcard character, X. A maximum of XX in a Call Park extension number (for example, 80XX) can be configured, which provides up to 100 Call Park extension numbers. When a call is parked, Cisco Unified Communications Manager chooses the next Call Park extension number that is available and displays that number on the phone.

Directed Call Park

Directed Call Park allows you to transfer a call to an available user-selected Directed Call Park number.



Directed call park numbers can be configured in the Cisco Unified Communications Manager Directed Call Park Configuration window. Configured Directed Call Park numbers exist clusterwide. Phones that support the Directed Call Park busy lamp field (BLF) can be configured to monitor the busy or idle status of specific Directed Call Park numbers. Users can also use the BLF to speed-dial a Directed Call Park number.

Cisco Unified Communications Manager can park only one call at each Directed Call Park number. To retrieve a parked call, a user must dial a configured retrieval prefix followed by the Directed Call Park number at which the call is parked. Configure the retrieval prefix in the Directed Call Park Configuration window.

The example in the slide shows how the Directed Call Park feature can be used, as follows:

1. Users A and B connect in a call.
2. To park the call, A presses the Transfer softkey (or Transfer button, if available) and dials Directed Call Park number 80 (for example) or presses the BLF button for Directed Call Park number 80 (if the phone model supports the BLF button).
3. User A either presses the Transfer softkey (or Transfer button) again or goes on hook to complete the Directed Call Park transfer. This action parks user A on Directed Call Park number 80.
4. From any phone with a correctly configured partition and CSS, user C dials the Directed Call Park prefix (21, for example) followed by the Directed Call Park number 80 to retrieve the call. User C connects to user B.
5. If the call is not retrieved before expiration of the Call Park Reversion Timer configured in the service parameter, the call reverts to the configured reversion number.

Directed Call Park Configuration

The Directed Call Park feature comes with Cisco Unified Communications Manager software.

Directed Call Park Configuration

Directed Call Park Information

Number*	8X
Description	Directed Call Park Range
Partition	hh_devices
Reversion Number	35
Reversion Calling Search Space	hh-cor-internal
Retrieval Prefix*	21

- Ensure that Directed Call Park number or range is unique within the cluster.
- The Reversion Number is the number to which the parked call will return if not retrieved.
- The Retrieval Prefix is needed to differentiate between park and retrieval.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-9

Any phone that can perform a transfer can use Directed Call Park. It does not require special installation.

To configure Directed Call Park, define a unique Directed Call Park number or a range of Directed Call Park numbers. A range must be specified by using wildcards. For example, the range 40XX configures the range as 4000 to 4099.

Caution Do not enter a range by using dashes (such as 4000–4040).

Note Only individual Directed Call Park numbers can be monitored with the Directed Call Park BLF. If a range of numbers is configured, the BLF cannot support monitoring of the busy or idle status of the range or of any number within the range.

Note Cisco recommends to not configure both Directed Call Park and the park softkey for Call Park in Cisco Unified Communications Manager, but the possibility exists to configure both. If both are configured, ensure that the Call Park and Directed Call Park numbers do not overlap.

To operate, Directed Call Park requires Cisco Unified Communications Manager 6.0 or later.

A user can park and retrieve a call by using Directed Call Park from any phone that can perform a transfer, including Cisco Unified IP Phones 7905, 7912, 7920, 7940, 7960, and 7970. Cisco VG248 Analog Phone Gateways also support Directed Call Park.

The following Skinny Client Control Protocol (SCCP) and SIP phones support Directed Call Park BLF: Cisco Unified IP Phones 7941, 7961, 7970, and 7971.

The following SCCP phones support Directed Call Park BLF:

- Cisco Unified IP Phones 7905, 7912, 7920, 7940, 7960
- Cisco Unified IP Phone Expansion Module 7914

Configuration of Call Park Button

Directed Call Park buttons and BLF can be configured for phones or user profiles.

Configuration of Call Park Button

Busy Lamp Field/Speed Dial Button Settings			
Destination	Directory Number	Label	Label ASCII
1 2180	< None >	DCP	DCP
2	< None >		

- Directed buttons BLF can be configured for phones or user profiles.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-10

To configure BLF/Directed Call Park buttons, access the Cisco Unified Communications Manager Administration and perform the following procedure:

- To configure the BLF/Directed Call Park button in the Phone Configuration window, find the phone.
- To configure the BLF/Directed Call Park button for user device profiles, find the user device.
- After the configuration window displays, click the **Add a new BLF Directed Call Park** link in the Association Information pane.

Tip

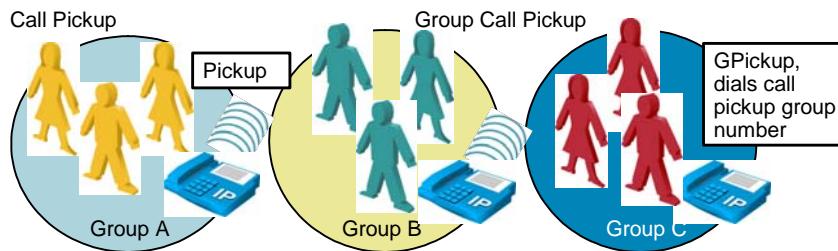
The link does not display in the Association Information pane if the phone button template that is applied to the phone or device profile does not support BLF/Directed Call Park.

-
- Configure the BLF/Directed Call Park button with the directory number, label, and ASCII label.
 - After the configuration is complete, click **Save** and close the window.

Call Pickup and Hold Reversion

This topic describes Call Pickup and Group Call Pickup features, as well as Hold Reversion.

Call Pickup and Group Call Pickup



- **Call Pickup**—Allows users to pick up incoming calls within their own group.
 - Cisco Unified CM automatically dials the configured call pickup group number when the user presses Pickup.
- **Group Call Pickup**—Allows users to pick up incoming calls from another group.
 - After pressing Gpickup button, user must enter the appropriate pickup group number.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-12

The purpose of Call Pickup is to enable a group of users who are seated near each other to cover incoming calls as a group. When a member of the group receives a call and is not available to answer it, any other member of the group can pick up the call from their own phone.

Three types of Call Pickup exist:

- **Call Pickup:** Enables users to pick up incoming calls on any telephone within their own group. When the users press the **Call Pickup** button or **PickUp** softkey, Cisco Unified Communications Manager automatically dials the appropriate Call Pickup number.
- **Group Call Pickup:** Enables users to pick up incoming calls on any telephone within their own group or in another group. Users press the **Group Call Pickup** button or **Gpickup** softkey and dial the appropriate group number for Call Pickup. Users manually enter a number with Group Call Pickup but not with Call Pickup because more than one group can exist and Cisco Unified Communications Manager needs to know which one to dial. With Call Pickup in effect, there is only one number corresponding to one group.
- **Other Group Call Pickup:** Allows users to pick up incoming calls in a group that is associated with their own group. This type of call pickup is covered in the next subtopic.

Example for Pickup and Group Pickup Function:

Phone A and Phone B are assigned to Call Pickup Group Support with the Number 4685. Phone C belongs to Call Pickup Group R&D with Number 4688.

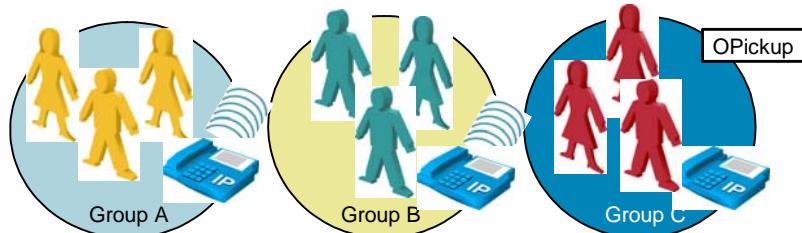
When phone C calls Phone A, and Phone A does not answer, Phone B goes off-hook, presses the PickUp softkey, and then presses the Answer softkey. The call is rerouted to Phone B.

When Phone B calls Phone C, and Phone C does not answer, Phone A goes off-hook, presses the More softkey, then the GPickup softkey, enters 4688, and then presses the Answer softkey. The call is rerouted to Phone A.

Other Group Call Pickup

This subtopic describes the Other Group Call Pickup feature.

Other Group Call Pickup



Group C is associated with Group A and B

- Allows users to pick up incoming calls in a group that is associated with their own group.
- Cisco Unified CM automatically searches for incoming calls in associated groups when the user activates this feature.
- Use the softkey OPickup.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-13

Other Group Call Pickup allows users to pick up incoming calls in a group that is associated with their own group. Cisco Unified Communications Manager automatically searches for incoming calls in the associated groups to make the call connection when the user activates this feature from a Cisco IP phone. Use the softkey **OPickup** for this type of call pickup.

When more than one associated group exists, the priority of answering calls for the associated group goes from the first associated group to the last associated group. For example, groups A, B, and C associate with group X, and the priority of answering calls goes to group A, then B, and then C.

Usually, within the same group, the longest alerting call (longest ringing time) is picked up first if multiple incoming calls occur in that group. For Other Group Call Pickup, priority takes precedence over the ringing time if multiple associated pickup groups are configured.

Both the idle and off-hook call states make the three softkeys, Pickup, GPickup, and OPickup, available.

Call Pickup, Group Call Pickup, and Other Group Call Pickup can be automated by enabling the service parameter **Auto Call Pickup Enabled**. When this parameter is enabled, Cisco Unified Communications Manager automatically connects users to the incoming call in their own pickup group, in another pickup group, or a pickup group that is associated with their own group after users press the appropriate softkey on the phone. This action requires only one keystroke. Auto Call Pickup connects the user to an incoming call. When the user presses a pickup softkey on the phone, Cisco Unified Communications Manager locates the incoming call and completes the call connection. If automation is not enabled, the user must press the softkeys **Pickup** and **Answer** to make the call connection.

Call Pickup Configuration

This subtopic describes how to configure Call Pickup.

The screenshot shows the 'Call Pickup Configuration' page under 'Call Routing > Call Pickup Group'. The 'Call Pickup Group Information' section contains fields for 'Call Pickup Group Name*' (Support), 'Call Pickup Group Number*' (4685), 'Description' (Support Group), and 'Partition' (< None >). Below this is the 'Associated Call Pickup Group Information' section, which includes a 'Find Pickup Numbers by Numbers/Partition' search interface. A dropdown menu for 'Partition' is set to '< None >'. A 'Call Pickup Group Numbers Contain' input field is empty. A 'Find' button is present. Below these is a list titled 'Available Call Pickup Groups' with the message '(No Matches Found)'. At the bottom is a blue 'Add to Associated Call Pickup Groups' button. The page footer includes copyright information and a reference to CIPT1 v6.0—5-14.

- Define a unique Call Pickup Group Number

This subtopic describes how to configure Call Pickup.

To configure Call Pickup, call pickup number must first be added and configured and then the number to the desired directory numbers assigned.

Follow this procedure to add a call pickup number and group in Cisco Unified Communications Manager Administration:

- Choose **Call Routing > Call Pickup Group**.
- To add a new Call Pickup Group, click **Add New**. The Call Pickup Group Configuration window displays.
- Enter a unique pickup group name and unique pickup group number.
- Access to call pickup groups can be restricted by assigning a partition to the call pickup group number. When this configuration is used, only the phones that have a CSS that includes the partition with the call pickup group number can participate in that call pickup group. Make sure that the combination of partition and group number is unique throughout the system.
- Assign the pickup group to a route partition as desired.
- To save the new call pickup group in the database, click **Save**.

Note	In the section Associated Call Pickup Group Information, pickup groups that should be associated with the current pickup group can be specified. The Other Group Call Pickup feature uses this list. The groups are searched sequentially, beginning with the first group in the list.
-------------	--

Call Pickup Configuration (Cont.)

Directory Number Configuration

Call Forward and Call Pickup Settings		
Voice Mail Destination		Calling Search Space
Forward All	<input type="checkbox"/> or <input type="text"/>	< None >
Secondary Calling Search Space for Forward All		< None >
Forward Busy Internal	<input type="checkbox"/> or <input type="text"/>	< None >
Forward Busy External	<input type="checkbox"/> or <input type="text"/>	< None >
Forward No Answer Internal	<input type="checkbox"/> or <input type="text"/>	< None >
Forward No Answer External	<input type="checkbox"/> or <input type="text"/>	< None >
Forward No Coverage Internal	<input type="checkbox"/> or <input type="text"/>	< None >
Forward No Coverage External	<input type="checkbox"/> or <input type="text"/>	< None >
Forward on CTI Failure	<input type="checkbox"/> or <input type="text"/>	< None >
No Answer Ring Duration (seconds)	<input type="text"/>	
Call Pickup Group	<input type="text"/>	<input type="button"/>

- Assign the Call Pickup Group to a line or directory number.

© 2008 Cisco Systems, Inc. All rights reserved.

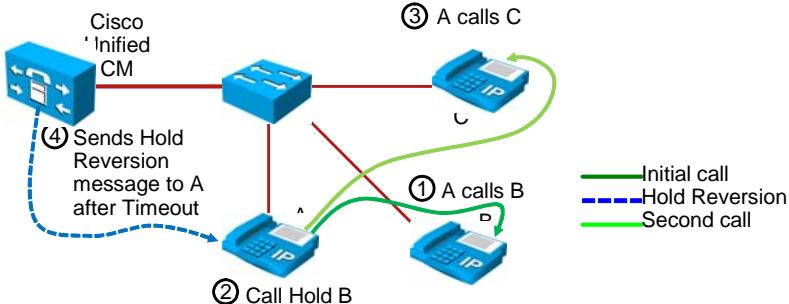
CIPT1 v6.0—5-15

After the call pickup group is added in Cisco Unified Communications Manager, the group is assigned to the desired line from the Directory Number Configuration window.

Hold Reversion

The Hold Reversion feature alerts a phone user when a held call exceeds a configured time limit.

Hold Reversion



- The Hold Reversion feature alerts a phone user when a held call exceeds a configured time limit.
- Alerts are generated, such as a ring or beep, at the phone to remind the user to handle the call.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-16

When the held call duration exceeds the limit, Cisco Unified Communications Manager generates alerts, such as a ring or beep, at the phone to remind the user to handle the call. The held call becomes a reverted call when the hold duration exceeds the configured time limit.

Hold Reversion can be configured for any directory number that is associated with a phone that is on the same Cisco Unified Communications Manager cluster. The phone device that is associated with the line must support this feature, or Hold Reversion does not activate. When multiple phone devices share a line, only those devices that support Hold Reversion can use this feature.

Note	Cisco Hold Reversion applies specifically to calls that an end user puts on hold. This feature cannot be activated on calls that the system or network puts on hold; for example, during conference or transfer operations.
-------------	---

The types of alerts that are generated at the phone for reverted calls depend on the capabilities of the phone device. Cisco Unified Communications Manager provides the following alerts when the Hold Reversion feature activates, depending on the capabilities of the phone and the firmware release that is installed:

- The phone rings once or beeps once.
- The status line briefly displays “Hold Reversion” for the reverted call at the user phone.
- The LED next to the line button flashes continuously on the phone handset, like other alerting operations.
- A “wobbling” handset icon displays for a reverted call.

Hold Reversion Configuration: Timer

Cisco Hold Reversion automatically installs when you install Cisco Unified Communications Manager.

The screenshot displays two configuration pages from Cisco CallManager:

- System > Service Parameters > Cisco CallManager**: Shows the "Clusterwide Parameters (Feature - Hold Reversion)" section. It includes fields for "Hold Reversion Duration" (set to 0), "Hold Reversion Notification Interval" (set to 30), and "CFA Destination Override" (set to True). A note indicates that a value of 0 will disable the feature.
- Call Routing > Directory Number**: Shows "Line Settings for All Devices". It includes fields for "Hold Reversion Ring Duration (seconds)" and "Hold Reversion Notification Interval (seconds)". Notes state that zero will disable the feature for both fields.

A callout box highlights the "Hold Reversion Duration" field in the first section, with the following text:

- The default Hold Reversion timeout is defined in the CallManager Service parameters and is overruled by a setting on the line.

After Cisco Unified Communications Manager is installed, Hold Reversion feature settings must be configured in Cisco Unified Communications Manager Administration to enable the feature.

Two timers in Cisco Unified Communications Manager specify the alert operations for hold reversion:

- The **Hold Reversion Duration** timer specifies the wait time before a reverted call alert gets issued to the phone of the holding party.
- The **Hold Reversion Notification Interval** timer specifies the frequency of the periodic reminder alerts to the holding party phone.

For example, a duration timer setting of 20 and an interval setting of 30 means that Cisco Unified Communications Manager will issue the first alert after 20 seconds and a reminder alert every 30 seconds thereafter. The Hold Reversion feature activates when the Hold Reversion Duration timer times out (after 20 seconds).

Perform the following procedure, which assumes that directory numbers are configured for a phone or that the phones are using autoregistration, to enable the Hold Reversion feature and to configure the Hold Reversion timer settings:

- To enable Hold Reversion for the cluster, change the Hold Reversion Duration timer in the Service Parameters window to a value greater than 0.
- If the default system setting for reminder alerts is not to be used, configure the Hold Reversion Notification Interval timer in the Service Parameters window. The default value specifies 30 seconds.
- To disable Hold Reversion for a line when the system setting is enabled, enter a value of 0 for the Hold Reversion Duration timer in the Directory Number Configuration window. If

the field is left empty, Cisco Unified Communications Manager uses the cluster timer setting.

- To enable Hold Reversion for a line when the system setting is disabled, set the Hold Reversion Duration timer in the Directory Number Configuration window to a value greater than 0. To enable reminder alerts, configure the Hold Reversion Notification Interval timer to a value greater than 0 in the same window or leave it blank to use the cluster setting.
- To configure Hold Reversion timer settings that differ from the cluster settings when Hold Reversion is enabled, enter different values for the Hold Reversion timers in the Directory Number Configuration window.

The parameters in the Clusterwide Parameters window are as follows:

- **Hold Reversion Duration:** This mandatory parameter specifies the number of seconds that a call remains on hold before Cisco Unified Communications Manager reverts the call back to the phone that placed the call on hold. When the value specified in this parameter expires, a Hold Reversion notification (audio or visual) occurs on the phone of the holding party until the call is answered or the value specified in the Maximum Hold Duration Timer service parameter expires. Be sure to specify a value in this parameter that is less than the value specified in the Maximum Hold Duration Timer service parameter; if a greater value is specified in this parameter, the Maximum Hold Duration Timer will expire first and the held call will be dropped. A value of zero disables the Hold Reversion feature. The default is 0 seconds, the minimum is 0 seconds, and the maximum is 1200 seconds.
- **Hold Reversion Notification Interval:** This mandatory parameter specifies the number of seconds that must elapse between notifications of a call on hold. When the time specified in the Hold Reversion Duration service parameter expires, Cisco Unified Communications Manager reverts the call back to the phone that placed the call on hold and reminds the user of the call on hold. Reminder notification occurs by either ringing the phone once, flashing the line and handset light once, or beeping once, depending on the phone state and the selections made in the Ring Setting of Busy Station and Ring Setting of Idle Station service parameters. The timer in this parameter resets after each notification and the notification occurs again when the specified interval elapses.

For example, if a phone has Beep Only configured for both Ring Setting parameters, the Hold Reversion Interval service parameter is set to 30 seconds, and a call is waiting on hold. When the Hold Reversion Duration service parameter expires, the phone will beep once every 30 seconds until the call is answered or the value specified in the Maximum Hold Duration Timer service parameter expires.

If Disable is selected for the Ring Setting parameter, no notification occurs when the Hold Reversion Interval expires. You can also disable the notification by setting this parameter to zero. If Ring is selected for the Ring Setting parameter, Cisco Unified Communications Manager converts that setting for hold calls only (no change to incoming call settings as specified by the Ring Setting parameters) to Ring Once and rings the phone only one time at the expiration of the Hold Reversion Interval (so that for calls reverting from hold, the phone will not ring continuously). The default is 30 seconds, the minimum is 0 seconds, and the maximum is 1200 seconds.

- **CFA Destination Override:** This mandatory parameter determines whether Cisco Unified Communications Manager ignores Call Forward All (CFA) destinations when the CFA destination is the same as the calling party number. For example, John (on Phone A) has CFA set to Jane (on Phone B). With this parameter enabled, Jane has the ability to transfer a call to John's phone without having that same call sent back to Jane due to John's CFA setting. This capability proves useful when Jane receives a call forwarded from John's phone, but which must go back to John's phone so that the caller can leave a voice message for John. If this parameter is set to False, Jane cannot send any calls to John's phone and the caller will not be able to leave a voice message for John.

Note	This override capability only works when the calling party number matches precisely with the number specified in the Call Forward All destination.
-------------	--

In cases where the calling party number has been transformed, the calling party number may not match the CFA destination and override will not be allowed. Valid values are True (CFA overrides are permitted) or False (CFA overrides are not permitted). The default is False.

Hold Reversion Configuration: Focus

When a phone has a reverted call and an incoming call alerting, the call focus priority specifies which call type has focus, meaning which call type has priority for user actions, such as going off-hook.

The screenshot shows the 'System > Device Pool' configuration page. The 'Device Pool Settings' section includes fields for 'Device Pool Name*' (set to 'HH-LAN'), 'Cisco Unified Communications Manager Group*' (set to 'Default'), 'Calling Search Space for Auto-registration' (set to '< None >'), and 'Reverted Call Focus Priority' (set to 'Default'). A red box highlights the 'Reverted Call Focus Priority' dropdown menu, which also contains the option 'Highest'.

▪ Revert Call Focus Priority specifies which call is connected, a new incoming call or the reverted call, when a user goes off-hook.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-18

At Cisco Unified Communications Manager installation, incoming calls have priority.

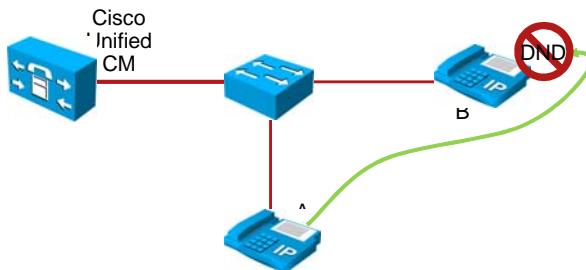
You can configure the Reverted Call Focus Priority setting for a device pool, which is then assigned to a phone device in Cisco Unified Communications Manager Administration. The focus priority for the device pool that is associated with the phone applies to reverted and incoming calls that appear on the same line or on different lines on the phone device.

Note	A priority value of Default means that incoming calls have priority, whereas a priority value of Highest means that reverted calls have priority.
-------------	---

Do Not Disturb, Intercom, and Cisco Call Back

This topic describes the three Cisco Unified Communications Manager features Do Not Disturb, Intercom, and Cisco Call Back.

Do Not Disturb (DND)



- Do Not Disturb (DND) feature allows you to turn off the ringer for an incoming call by pressing a feature button, softkey, or using the User Options web page.
- Users can choose to have the Cisco Unified IP phone beep or flash to indicate an incoming call.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-20

The DND feature allows you to turn off the ringer for an incoming call. When DND is enabled, you can choose to have the Cisco Unified IP phone beep or flash to indicate an incoming call. You can configure DND directly from your Cisco Unified IP phone or from the User Option web pages.

When DND is enabled, all new incoming calls with normal priority will honor the DND settings for the device. High-priority calls, such as Cisco Emergency Responder calls or calls with MLPP, will ring on the device. Also, when you enable DND, the Auto Answer feature becomes disabled.

You can enable and disable DND by any of the following methods:

- Softkey
- Feature line key
- Cisco Unified Communications Manager User Option web pages

You can also enable and disable DND on a per-phone basis in Cisco Unified Communications Manager Administration.

When DND is enabled, the Cisco Unified IP phone displays the message Do Not Disturb Is Active. The DND line button icon also turns into an empty circle, and the light turns amber (only on phones that have IP phone buttons supporting lights) when DND is active.

DND incoming call alert settings determine how the incoming call alert gets presented to the user when DND Ringer Off is enabled. The available options are as follows:

- **Disable:** This option disables both beep and flash notifications of a call, but incoming call information still gets displayed.
- **Beep Only:** For an incoming call, this option causes the Cisco Unified IP phone to play a beep tone only.
- **Flash Only:** For an incoming call, this option causes the Cisco Unified IP phone to display a flash alert only.

You can configure DND Incoming Call Alert on a per-device basis and also in the Common Phone Profile window for group settings. If the configuration is not set up at the device level, the Common Phone Profile settings are used.

Do Not Disturb Configuration: Common Profile

Do Not Disturb comes with Cisco Unified Communications Manager software. It does not require special installation.

DND Configuration: Common Profile

Device > Device Settings > Common Phone Profile

Common Phone Profile Configuration

Related Links: Back To Find/List Go

Common Phone Profile Information

Name*	Standard Common Phone Profile
Description	Standard Common Phone Profile
Local Phone Unlock Password	[Redacted]
DND Option*	Ringer Off
DND Incoming Call Alert*	Beep Only
Phone Personalization*	Default
<input checked="" type="checkbox"/> Enable End User Access to Phone Background Image Setting	

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-21

DND can be configured on a per-phone basis or by using a common phone profile.

To configure DND on a particular Cisco Unified IP phone, navigate to **Device > Phone** and choose the phone that you want to configure. In the Do Not Disturb pane on the Phone Configuration window, configure the parameters Do Not Disturb-checkbox, DND Option, and DND Incoming Call Alert.

To add DND to a common phone profile, navigate to **Device > Device Settings > Common Phone Profile** and choose the phone profile that should be modified. In the Common Phone Profile Configuration window, configure the DND parameters DND Option and DND Incoming Call Alert.

Do Not Disturb Configuration: Add DND Softkey

Default softkey templates do *not* make a DND softkey available.

DND Configuration: Add DND Softkey

Device > Device Settings > Softkey Template

Softkey Layout Configuration
Softkey Template: Standard Feature 2
Select a call state to configure On Hook

Unselected Softkeys

- Call Back (CallBack)
- Conference List (ConfList)
- Direct Transfer (DirTrfr)
- Group Pick Up (GPickUp)
- HLog (HLog)
- Immediate Divert (iDivert)
- Join (Join)
- MeetMe (MeetMe)
- Mobility (Mobility)
- Other Pickup (oPickup)
- Pick Up (PickUp)
- Quality Report Tool (QRT)
- Remove Last Conference Party (RmLstC)
- Select (Select)
- Undefined (Undefined)
- Video Mode Command (VidMode)

Selected Softkeys (ordered by position)**

- Redial (Redial)
- **NewCall (NewCall)
- Forward All (CfwdAll)
- Toggle Do Not Disturb (DND)

► ▲ ▼ ◀

A DND softkey has to be added to the phones Softkey Template in order to let the user control the DND state.

A feature key can also be used to control DND state.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-22

To add a DND softkey, navigate to **Device > Phone Settings > Softkey Template**, add a device to a softkey template in the Softkey Template Configuration window, and associate the template to the device.

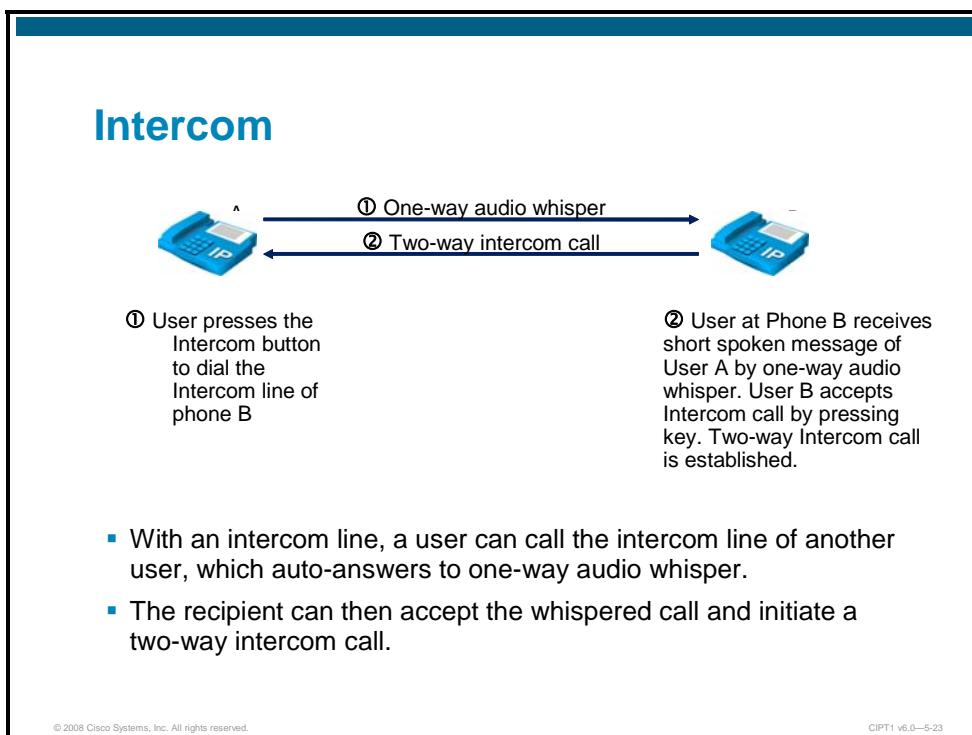
A DND softkey is available in the following states:

- Connected
- Connected Conference
- Connected Transfer
- Off Hook
- OffHook with Feature
- On Hold
- Remote In Use
- On Hook
- Ring In
- Ring Out
- Digits After First

To configure a DND feature key, navigate to **Device > Device Settings > Phone Button Template** and add Do Not Disturb in the Phone Button Template Configuration window.

Intercom

Intercom, a new type of phone line, combines the functionality of a traditional line and a speed dial.



With an intercom line, you can call the intercom line of another user, which auto-answers to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call.

You can use an intercom line to dial any other intercom line, or you can preconfigure the line to a single specific target intercom line.

Note You can use an intercom line only to dial other intercom lines.

Intercom allows you to place a call to a predefined target. The called destination auto-answers the call in speakerphone mode with mute activated. This sets up a one-way voice path between the initiator and the destination, so the initiator can deliver a short message, regardless of whether the called party is busy or idle.

To ensure that the voice of the called party does not get sent back to the caller by the automatically answered intercom call, Cisco Unified Communications Manager implements whisper intercom, which means that only one-way audio exists from the caller to the called party until the called party accepts the intercom call by pressing the intercom phone button. Only then does the call turn into a full two-way audio call.

Note An auto-answer tone will mark the beginning of the whisper state for both the sender and the recipient.

Intercom is supported on the following phone models: Cisco Unified IP Phone 7931 (SCCP only), 794[125], 796[125], and 797[015].

Intercom Configuration Steps

There are four steps to be taken to configure the Intercom feature.

Intercom Configuration Steps

1. Create intercom partition.
2. Verify automatically created intercom CSS or (optionally) replace by customized intercom CSS.
3. Create intercom directory numbers.
4. Assign intercom directory numbers to phones.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-24

Follow these steps to configure the Intercom feature:

Step 1 Create an intercom partition.

Note When you create an intercom partition, the administration user interface will automatically generate a corresponding intercom CSS with the same name (extended by the text “_GEN” that includes this new intercom partition).

Step 2 Verify the automatically generated intercom CSS, or, optionally, replace it with a customized intercom CSS.

Note Customized intercom CSSs are only required if an intercom phone button should support multiple intercom targets and if access control is required in order to limit the targets that are available to the intercom phone button. The automatically generated intercom CSS does not need to be changed for a standard implementation of point-to-point intercom lines.

Step 3 Create the intercom directory numbers.

Step 4 Assign intercom directory numbers to phones.

Step 1: Create Intercom Partition

First, the intercom partition needs to be created.

The screenshot shows the 'Cisco Unified CM Administration: Call Routing > Intercom > Intercom Route Partition' screen. A callout box points to the 'Name' field, which contains the value 'Intercom, Intercom Phone1-Phone2'. The text inside the callout box states: 'Intercom partitions are created the same way as standard partitions.'

Add new Intercom Partition(s) Related Links: Back To Find/List Go

Intercom Partition Information

To enter multiple partitions, use one line for each partition entry. You can enter up to 1475 characters per partition. The names and descriptions can have up to a total of 1475 characters. The partition name must be at least 1 character long and cannot exceed 50 characters. Use a comma (',') to separate the partition name and description on the same line. If the description is not entered, Cisco Unified Communications Manager uses the partition name as the description. For example:
<< partitionName >> , << description >>
CiscoPartition, Cisco employee partition
DallasPartition

Name: *

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-25

Go to **Call Routing > Intercom > Route Partition** to add one or more intercom partitions. Intercom partitions are created in the same way as normal partitions. Just enter the partition name and description separated by a comma. Assuming standard point-to-point intercom lines, one intercom partition is required per intercom line.

Step 2: Create Intercom CSS

After creating one or more intercom partitions, one intercom CSS is automatically created per intercom partition. If required, intercom CSSs can be customized manually.

Step 2: Verify Automatically Generated Intercom Calling Search Space

Cisco Unified CM Administration: Call Routing > Intercom > Intercom Calling Search Space

Automatically created intercom CSS
Name and description are taken from intercom partition ("..._GEN" added at the end)

Automatically created intercom CSS includes the previously configured intercom partition

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-26

To manage intercom CSSs, go to **Call Routing > Intercom > Intercom Calling Search Space**. This is only required if an intercom phone button should support multiple intercom targets and if access control is required in order to limit the targets that are available to the intercom phone button. The figure shows the automatically created intercom CSS that was created after the partition has been added in the previous step.

Step 3: Create Intercom Directory Numbers

The next step is to create intercom directory numbers.

Step 3: Create Intercom Directory Numbers

Cisco Unified CM Administration: Call Routing > Intercom > Intercom Directory Number

DN = directory number

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-27

To create intercom directory numbers, go to **Call Routing > Intercom > Intercom Directory Number** and click **Add New**. An intercom directory number range (from and to values) must be specified. The *from* and *to* values can be the same if only one intercom directory number should be added. For a point-to-point intercom line, a range of two directory numbers is specified. Select the intercom partition and enter a description and alerting name. Finally, choose an intercom CSS.

If the range was not limited to a single directory number, the entered description and alerting names should not be specific per intercom endpoint (because they are the same for all directory numbers of the range), or these values should be changed on the individual directory numbers after the range has been added.

- Note** After adding the intercom directory number range, each individual intercom directory number is shown in the list of intercom directory numbers and can be configured on its own. The intercom range is only a configuration tool to add multiple intercom directory numbers with similar settings in a single step.

Step 4: Assign Intercom Directory Numbers to Phones

In the last step, the intercom directory numbers are assigned to phone intercom lines.

Step 4: Assign Intercom Directory Number to Phone

Phone Configuration Page -> Intercom Line

Intercom Directory Number Configuration

Intercom Directory Number Information	
Intercom Directory Number*	9801
Route Partition*	Intercom
Description	Intercom Phone1-Phone2
Alerting Name	Phone1
ASCII Alerting Name	Phone1
Intercom Directory Number Settings	
Calling Search Space*	Intercom_GEN
Presence Group*	Standard Presence group
Auto Answer*	Auto Answer with Speakerphone

Enter the intercom DN to be applied to the phone intercom line

Configuration of intercom DN is loaded after intercom directory number has been entered

DN = directory number

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-28

To assign an intercom directory number to a phone, go the phone configuration page and click the intercom line to which you want to assign the intercom directory number.

Note

An intercom directory number is assigned to an intercom phone button. If the phone does not yet have a phone button template with an intercom line, the phone must be configured appropriately.

In the Intercom Directory Number Configuration window, enter the Intercom Directory Number that should be assigned to the intercom line. After the intercom directory number has been entered, the configuration of the previously configured intercom directory number is loaded. Any changes that are done to the values shown in the figure reconfigure the intercom directory number. These values include the intercom partition, alerting name, and intercom CSS.

Step 4: Assign Intercom Directory Number to Phone (Cont.)

Intercom Directory Number Configuration

Line 1 on Device SEP00070E576F43

Display (Internal Caller ID) Display text for a line appearance is intended for displaying text such as a name instead of a directory number for internal calls. If you specify a number, the person receiving a call may not see the proper identity of the caller.

ASCII Display (Internal Caller ID)

Line Text Label

ASCII Line Text Label

Speed Dial

External Phone Number Mask

Configure line appearance of intercom DN.

If Speed Dial is entered, pressing intercom phone button creates intercom connection to specified intercom DN (used for point-to-point intercom DN).

If no Speed Dial is set, target intercom DN has to be dialed after pressing intercom phone button.

DN = directory number

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-29

The line appearance of the intercom directory number is not stored with the intercom directory number, but at the individual phone intercom line. Therefore all fields are blank and the entered values do not update the intercom directory number itself, but only the intercom line appearance at the currently configured phone. Enter the Display text (that is, how an intercom call from this intercom line is shown at the receiving phone) and the line text label that should be shown next to the intercom phone button inside the phone display.

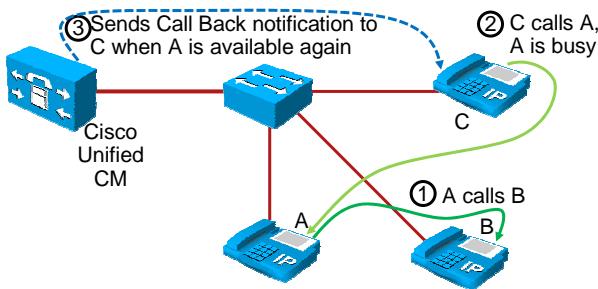
Finally, you can enter a speed dial. The speed dial is the target of the intercom connection (that is, any other intercom directory number). If no speed dial is entered, the target intercom directory number must be dialed after pressing the intercom phone button. If a speed dial is configured, the intercom connection is immediately created after the user presses the intercom phone button.

-
- Note** Instead of configuring intercom directory numbers from **Call Routing > Intercom > Intercom Directory Number** and then assigning the existing intercom directory number to a phone intercom line, the intercom directory number can be created from the intercom line configuration page of a phone by entering an intercom directory number that does not exist yet. In this case, all intercom directory number values will be blank, and after the intercom directory number has been configured, the directory number portion is saved as a new intercom directory number and the line appearance configuration is stored at the phone intercom line. The same concept applies to phone directory numbers; they can be created by going to **Call Routing > Directory Number** or from a phone line.
-

Cisco Call Back

This subtopic describes the Cisco Call Back feature.

Cisco Call Back



- Receive callback notification when a called party becomes available.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-30

The Cisco Call Back feature allows receiving callback notification on a Cisco Unified IP phone when a called-party line becomes available. To receive callback notification, a user presses the CallBack softkey upon receiving a busy or ringback tone. Callback notification can be activated on a line on a Cisco Unified IP phone in a Cisco Unified Communications Manager cluster. Callback notification cannot be activated if the called party has forwarded all calls to another extension (CFA feature).

Example: Cisco Call Back

IP phone user C calls IP phone user A in the same cluster. If IP phone A is busy or there is no answer, IP phone user C activates the Cisco Call Back feature through the CallBack softkey. When IP phone A becomes available, IP phone C receives an audible alert and visual notification that the previously dialed number became available. Cisco Unified Communications Manager remembers the dialed number, so IP phone user C can then press the Dial softkey to reach IP phone user A.

Cisco Call Back Configuration

This subtopic describes the configuration of the Cisco Call Back feature.

Cisco Call Back Configuration

Device > Device Settings > Softkey Template

Sofkey Layout Configuration
Sofkey Template: Modified Standard Feature
Select a call state to configure: On Hook

Unselected Softkeys	Selected Softkeys (ordered by position)**
Conference List (ConfList) Direct Transfer (DirTrf) Group Pick Up (GPickUp) Immediate Divert (IDivert) Join (Join) Meet Me (MeetMe) Other Pickup (oPickup) Pick Up (PickUp) Quality Report Tool (QRT) Remove Last Conference Party (RmLstC) Select (Select) Undefined (Undefined) Video Mode Command (VidMode)	Redial (Redial) **NewCall (NewCall) Forward All (CfwdAll) Call Back (CallBack)

▪ Add softkey to the phones softkey template

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-31

The phone states that support Cisco Call Back are Busy, Call Forward Busy, or No Answer. The No Answer state could include Call Forward No Answer to a voice-mail system or to another extension.

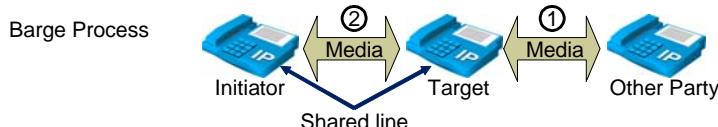
To configure Cisco Call Back, choose the softkey template (for example, the Standard User template), copy and insert the template, and name it something appropriate, such as Standard User Callback. Next, configure the softkey layout by choosing the On Hook call state and the Call Back option. Then, choose Ring Out, include the Call Back option by making sure that it is at the top of the list, and click **Save**.

Barge and Privacy

This topic discusses how to configure Barge and Privacy settings.

Barge and Privacy Overview

- **Barge:** Users can add themselves to remotely active calls on shared line.
 - Barge uses built-in conference bridge; cBarge uses shared conference bridge.
- **Privacy:** Users can allow or disallow other users on shared line to view call information or to use Barge or cBarge.



1. Original two-party call
2. Initiator barges into the call → three-way call:
 - If initiator hangs up, original call remains active.
 - If target hangs up, initiator and other party connect point-to-point.
 - If other party hangs up, original call and barged call are released.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-33

The Barge feature allows users to add themselves to an existing call on a shared line.

These two types of Barge are available in Cisco Unified CallManager Release 4.0 and later:

- **Barge using built-in conference:** (Barge softkey) Barge uses the built-in conference capability of the target IP phone. Barge also uses the Standard User or Standard Feature softkey template (both contain the Barge softkey). When a Barge is being set up, no media interruption occurs and the only display change to the original call is a spinning circle that is displayed at the right side of the prompt status message window at the target device.
- **Barge using shared conference:** (cBarge softkey) Conference Barge (cBarge) uses a shared conference bridge. No standard softkey template includes the cBarge softkey. To allow users to access the cBarge softkey, you must add it to a nonstandard softkey template and then assign the softkey template to a device.

When a user presses the cBarge softkey, a Barge call is set up by means of the shared conference bridge, if it is available. The original call is split and then joined at the conference bridge, which causes a brief media interruption. The call information for all parties changes to Barge. The barged call becomes a conference call with the Barge target device as the conference controller. The conference controller can add more parties to the conference or can drop any party.

Note	The Conference, Join, Meet-Me, and cBarge features differ in their conferencing features. Conference (or ad-hoc conference) allows you to initiate a conference by calling each participant. Join allows you to connect current callers who are on a single line by creating a conference call. Meet-Me allows you to call a predetermined number at a scheduled time to host or join a conference. cBarge allows you to establish a conference by adding yourself to a call on a shared phone line.
-------------	--

When only two parties are left in the conference, they experience a brief interruption and then are reconnected as a point-to-point call, which releases the shared conference resources. When the initiator uses Barge to join the call, it becomes a three-way call. If the initiator hangs up, the original call remains active. If the target hangs up, the caller who used Barge and the other party connect in a point-to-point call. If the other party hangs up, the original call and the barged call are released.

The Privacy feature was introduced in Cisco Unified CallManager Release 4.0. With Privacy, administrators can enable or disable the ability of users with telephones that share the same line to view call status and to barge the call. Administrators enable or disable Privacy for each telephone.

Shared Line Appearance

Both Barge and Privacy features work only with shared lines.

The screenshot shows the 'Shared Line Appearance' configuration window. It includes fields for Directory Number Information (Number: 1000, Partition: < None >, Description: Shared Line), ASCII Alerting Name, and a checked checkbox for 'Allow Control of Device from CTI'. Below this is a table titled 'Associated Devices' containing two entries: SEP000FFE28FFD6 and SEP000B6A409C40. Buttons for 'Edit Device' and 'Edit Line Appearance' are at the bottom right. A red box highlights the list of associated devices.

- Some directory numbers can be associated with more than one device.

Cisco Unified Communications Manager considers a directory number on more than one device in the same partition to be a shared line appearance. One example of a shared line appearance is when a directory number appears on line 1 of a manager telephone and also on line 2 of an assistant telephone. Another example of a shared line would be a single incoming 800 number that is set up to appear as line 2 on every help desk telephone in an office.

These guidelines are helpful when using shared line appearances with Cisco Unified Communications Manager:

- A shared line appearance can be created by assigning the same directory number and partition to different lines on different devices.
- If other devices share a line, the words “Shared Line” are displayed in red next to the directory number in the Directory Number Configuration window in Cisco Unified Communications Manager Administration.
- If you change the CSS, Call Waiting, Call Forward, or Pickup settings on any device that uses the shared line, the changes are applied to all of the devices that use that shared line.
- To stop sharing a line appearance on a device, you can change the directory number or partition number for the line and update the device. (Deletion removes the directory number on the current device only. The deletion does not affect the other devices.)
- Do not use shared line appearances on any Cisco Unified IP phone that will be used with the Attendant Console.
- Do not use shared line appearances on any Cisco Unified IP Phone 7960 or 7961 that requires the Auto Answer capability.

Barge Configuration

This subtopic describes basic Barge configuration.

Barge Configuration

Enable clusterwide (Cisco CallManager Service Parameter)

The screenshot shows the 'Clusterwide Parameters (Device - Phone)' section of the Cisco CallManager Service Parameters window. A red box highlights the 'Built-In Bridge Enable' field, which has a dropdown menu open showing 'Off', 'On', and 'True' options. The 'True' option is selected and highlighted with a blue background.

Enable at device level

The screenshot shows the 'Device Configuration' window for a specific device. A red box highlights the 'Built In Bridge' field, which has a dropdown menu open showing 'Default', '< None >', 'Off', and 'On' options. The 'On' option is selected and highlighted with a blue background.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-35

To configure Barge with the built-in conference bridge, follow these steps:

- Assign the Standard User or Standard Feature softkey template (both contain the Barge softkey) to each device that accesses Barge by using the built-in conference bridge.
- To enable Barge clusterwide for all users, choose **System > Service Parameters** for the Cisco CallManager service and set the Built-In Bridge Enable clusterwide service parameter to On. Alternatively, configure Barge for each telephone by setting the Built In Bridge field in the Phone Configuration window on the device itself.
- Set the Party Entrance Tone to **True** if you desire tones when a Barge occurs.

To configure Barge with Shared Conference Bridge (cBarge), follow these steps:

- Assign the Standard User or Standard Feature softkey template (you configure cBarge to either template) to each device that accesses Barge by using the shared conference bridge.
- Set the optional clusterwide service parameter Party Entrance Tone to **True** (required for tones).
- In the End User Configuration window for each user who is allowed to access the cBarge with the cBarge feature, associate the device that has the cBarge softkey template that is assigned to it.
- Notify users that the cBarge feature is available.

Note	When the existing call uses G.711 and the barge initiator is only allowed to use G.729, cBarge has to be used because an initiator cannot barge into a G.711 call with G.729 using the built-in conference bridge.
-------------	--

Privacy Configuration

Recall that when Privacy is enabled, users on a shared line can enable or disable the capability of other users on the shared line to view call status and to barge the call.

The screenshot shows the 'Privacy Configuration' page with two main sections: 'Enable clusterwide' and 'Enable at device level'.

Enable clusterwide: This section contains four dropdown menus:

- Ring Setting of Busy Station ***: Beep Only
- Ring Setting of Idle Station ***: Ring
- Privacy Setting ***: True (highlighted with a red box)
- SIP Station KeepAlive Interval ***: 120

Enable at device level: This section contains several dropdown menus and a table:

- Location ***: Hub_None
- User Locale**: < None >
- Network Locale**: < None >
- Built In Bridge ***: Default
- Privacy ***: Default (highlighted with a red box)
- Owner User ID**: < None >
- Phone Load Name**: Off, On, Default (highlighted with a blue box)

A note at the bottom left says: "© 2008 Cisco Systems, Inc. All rights reserved." A note at the bottom right says: "CIPT1 v6.0—5-36"

To configure Privacy, follow these steps:

Step 1 Set the optional Privacy Setting clusterwide service parameter to **True**.

Note Do not set this parameter if only a few users need access to Privacy (see Step 3).

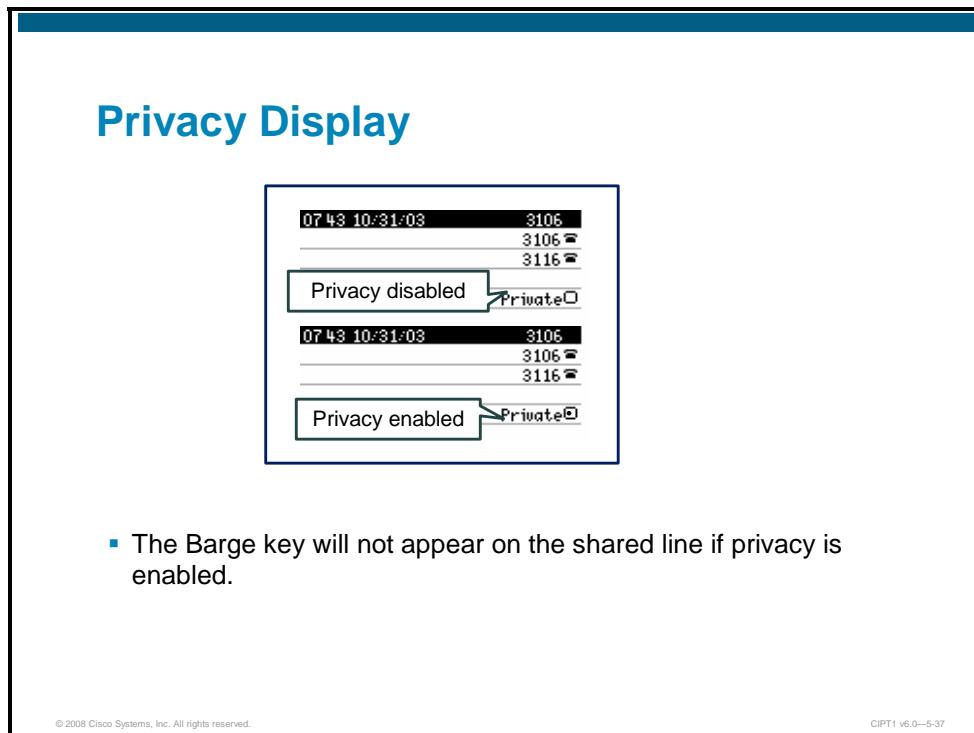
Step 2 For each phone button template for which Privacy should be enabled, add Privacy to one of the feature buttons.

Step 3 For each telephone user who wants to enable Privacy, choose **On** in the Privacy drop-down menu in the Phone Configuration window. If Privacy is configured clusterwide, the Privacy setting should be left at Default or set to **Off** to selectively disable privacy.

Step 4 For each telephone user who wants to enable Privacy, choose the phone button template that contains the Privacy feature button that was created in Step 2.

Privacy Display

The figure shows the phone display when the Privacy feature is assigned to a feature button.



When Privacy is enabled, the Privacy button display changes—a black circle appears inside the Privacy field. Now, when the other user on the shared line goes off hook on the shared line, the Barge softkey does not appear.

User Options Web Pages

This topic describes the functions and the configuration of the Cisco Unified Communications Manager User Options web page.

User Options Web Page

- Controllable features vary by phone model
- Some user-definable settings are:
 - User locale
 - User password
 - Do Not Disturb (On/Off)
 - Call Forward (All, On Busy, On No Answer, On No Coverage)
 - Message Waiting Indicator and Ring settings
 - Line text label
 - Speed dials
 - IP phone services and service buttons
 - Personal address book

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-39

Cisco Unified IP phone users can access the Cisco Unified Communications Manager User Options web page at <https://<CUCM Name or IP>/CCMUser/>, so that they can configure a variety of features on their phone.

Some user-definable settings are the following:

- User locale
- User password
- Do Not Disturb (On/Off)
- Call Forward (All, On Busy, On No Answer, On No Coverage)
- Message Waiting Indicator and Ring settings
- Line text label
- Speed dials
- Cisco IP Phone Services and service buttons
- Personal address book

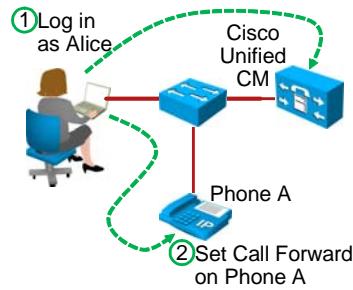
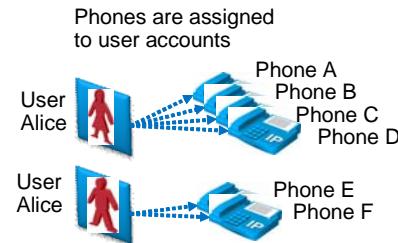
Which of these features are controllable depends on the phone model used.

In the Cisco Unified Communications Manager Enterprise Parameters, you can configure which features are made available to users by setting enterprise parameters as either True or False. For example, you can set the Show Speed Dial Settings enterprise parameter to False, and users cannot configure speed dials on their phones.

User Options Web Page: Phone to User Relation

The User Options web page allows users to configure their phones.

User Options Web Page: Phone to User Relation



- The User Options web page allows users to configure their phones.
- Phones are assigned to user accounts.
- Authenticated user is able to control the phones assigned.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-40

The phones configured by specific users must be assigned to the user accounts of those users. This assignment must be done using the Cisco Unified Communications Manager Administrator at **User Management > End User**, with the “Device Association” option.

User Options Example

A user wanting to change the Call Forward All setting for a specific phone must have this phone assigned to its personal user account by the administrator.

User Options Example



The screenshot shows the Cisco Unified Communications Manager User Options web page. The title bar says "User Options". Below it is a toolbar with "Line Settings Configuration", "Related Links", "Back To Find/List", and "Go". There are buttons for "Save", "Device", "Speed Dial", "Phone Services", and "Service URL". The main area has sections for "Status" (Status: Ready) and "Line Information" (Line: 90135 - Line 1). The "Incoming Call Forwarding" section contains several configuration options with checkboxes and radio buttons. One option, "Forward all calls to This Number 918415554321", has a red box around it, indicating it is being selected or highlighted. Other options include "When the line is busy, forward external calls to Voice Mail or This Number", "When the line is busy, forward internal calls to Voice Mail or This Number", and "When there is no answer, forward external calls to Voice Mail or This Number".

- Alice accesses <https://CUCM101/CCMUser/>.
- She logs in and she selects the phone A.
- Selects line settings and changes the CFA setting for phone A.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-41

The user accesses the Cisco Unified Communications Manager User Options web page at the URL <https://<CUCL Name or IP>/CCMUser/> .

After authentication, the user identifies the device ID and is able to select the line settings. The user is now able to change the forwarding settings of all the lines of the controlled device.

Cisco IP Phone Services

This topic describes the functions and configuration of the Cisco Unified Communications Manager IP Phone Services.

IP Phone Services

- Cisco Unified IP Phone Services are applications that utilize the web client or server and XML capabilities of the Cisco Unified IP phone
- Phone service applications provide value-added services by running directly on the user desktop phone
- Functions of a service application using IP Phone Services are
 - display of data (text and graphics)
 - user input
 - authentication
 - a mix of those functions
- Common examples for IP Phone Services are stock tickers, meal of the day, Cisco Extension Mobility, internet news readers

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-43

Cisco Unified IP Phone Services are applications that utilize the web client and/or server and Extensible Markup Language (XML) capabilities of the Cisco Unified IP phone. The Cisco Unified IP phone firmware contains a micro-browser that enables limited web browsing capability. These phone service applications provide the potential for value-added services and productivity enhancement by running directly on the user's desktop phone. For purposes of this chapter, the term phone service refers to an application that transmits and receives content to and from the Cisco Unified IP phone.

The following phones support Cisco IP Phone Services:

- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phones 7940G, 7941G and 7941G-GE
- Cisco Unified IP Phones 7960G, 7961G and 7961G-GE
- Cisco Unified IP Phones 7970G, and 7971G-GE

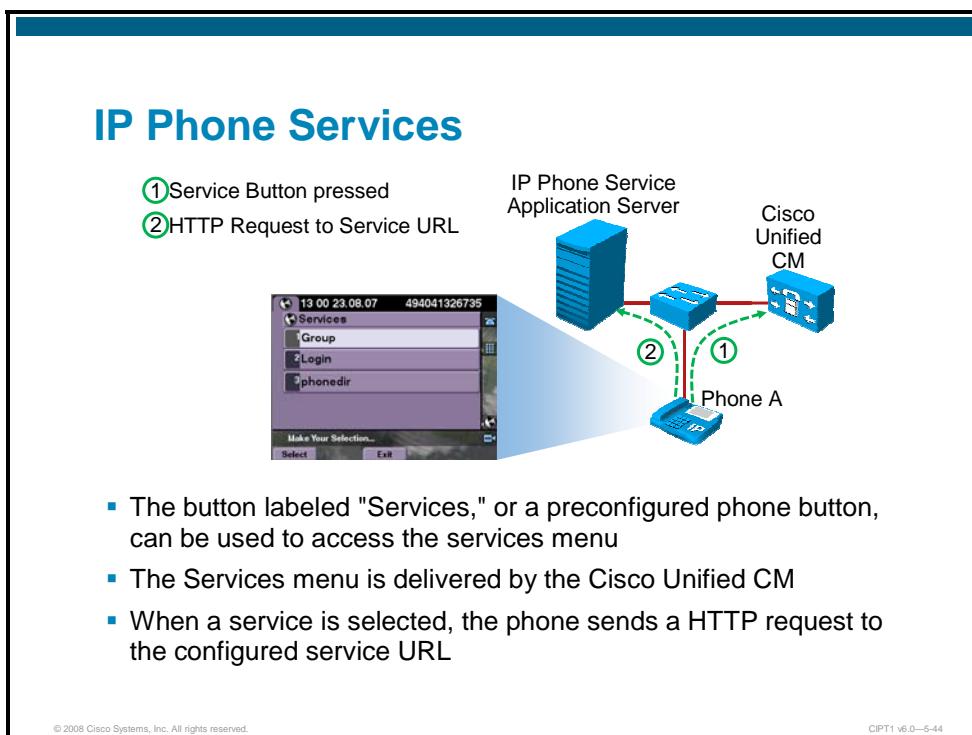
Cisco IP Phone Services can also run on the following IP phones; however these phone models support only text-based XML applications:

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phones 7912G and 7912G-A
- Cisco Unified Wireless IP Phone 7920

All of the IP phones listed above can process a limited set of Cisco-defined XML objects for enabling the user interface between the phone and the web server that contains the running phone service. Note that the phones listed above support phone services for both the SCCP and SIP.

Cisco IP Phone Services

Cisco IP Phone Services comprise XML applications that enable the display of interactive content with text and graphics on Cisco Unified IP phones.



Note	Cisco Unified IP Phone Services support Cisco Unified IP Phones 7970, 7960, 7940, 7912, and 7905 models.
-------------	--

A user can access a service from the supported phone model in two ways, either by pressing the **Services** button or using a preconfigured phone button. When the user presses the **Services** button, the phone uses its HTTP client to load a specific URL that contains a menu of services to which the user has subscribed. The user then chooses a service from the listing. When a service is chosen from the menu, the URL is requested via HTTP and a server provides the content, which then updates the phone display.

Typical services that might be supplied to a phone include weather information, stock quotes, and news quotes. Deployment of Cisco Unified IP Phone Services occurs using the HTTP protocol from standard web servers such as Microsoft Internet Information Server (IIS).

Users can only subscribe to services that are configured through Cisco Unified Communications Manager Administration. The following information is configured for each service:

- URL of the server that provides the content
- Service name and description, which helps end users browsing the system
- A list of parameters that are appended to the URL when it is sent to the server

These parameters personalize a service for an individual user. Examples of parameters include stock ticker symbols, city names, zip codes, or user IDs.

From Cisco Unified Communications Manager Administration, a lobby phone or other shared device can also subscribe to a service.

After the system administrator configures the services, users can log in to the Cisco Unified IP Phone User Options and subscribe to services. From Cisco Unified IP Phone User Options, users can subscribe to any service on their phone. Subscriptions occur on a per-device basis. Users can also add and update the service URL button.

Users can also subscribe to services from Cisco Unified Communications Manager Administration and from the Cisco Unified Communications Manager Bulk Administration Tool (BAT) application.

When the user clicks **Subscribe**, Cisco Unified Communications Manager builds a custom URL and stores it in the database for this subscription. The service then appears on the device services list.

Guidelines and Tips

A Cisco Unified IP phone displays graphics or text menus, depending on how the services are configured.

The Cisco Unified IP Phone 7960 supports the HTTP header that is sent with any window that includes a Refresh setting. Therefore, a new window can, after a fixed time, replace any XML object that displays. The user can force a reload by quickly pressing the **Update** softkey. If a timer parameter of zero was sent in the header, the window only moves to the next window when you press the **Update** softkey. The window never automatically reloads.

The Cisco Unified IP Phone 7960 supports the following softkeys that are intended to help the data entry process:

- **Submit:** This softkey indicates that the form is complete and that the resulting URL should be sent via HTTP.
- <<: Use the backspace softkey to backspace within a field.
- **Cancel:** This softkey cancels the current input.

Use the vertical scroll button for field-to-field navigation.

Caution	Do not put Cisco Unified IP Phone Services on any Cisco Unified Communications Manager server at a local site or any server that is associated with Cisco Unified Communications Manager, such as the TFTP server or directory database publisher server. This precaution eliminates the possibility that errors in a Cisco Unified IP Phone Service application will have an impact on Cisco Unified Communications Manager performance or interrupt call-processing services.
----------------	---

Cisco IP Phone Services Configuration Steps

This subtopic describes the configuration steps for Cisco IP Phone Services.

Cisco IP Phone Services Configuration Steps

1. Choose **Device > Device Settings > Phone Services**
2. Perform one of the followings tasks:
 - To add an Cisco IP phone service, click the **Add New** button
 - To update a service, click the name of the Cisco IP Phone Service that you want to update
3. Enter the appropriate settings for the service and save.
4. To apply the changes, update the IP Phone Services Configuration window.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-45

Follow these steps to add or update a Cisco IP Phone Service:

1. Access the Cisco Unified Communications Manager Administrator and choose **Device > Device Settings > Phone Services**.
The Find and List IP Phone Services window displays.
2. Perform one of the following tasks:
 - To add an IP phone service, click the **Add New** button. The IP Phone Services Configuration window displays. Continue with Step 3.
 - To update an existing IP phone service (for example, to change the service URL or other information), locate the appropriate IP phone service. Click the name of the IP phone service that you want to update and continue with Step 3.
3. Enter the appropriate settings for the service and click **Save**. Add, update, or delete parameters as needed.
4. To apply the changes, update the IP Phone Services Configuration window:
 - If the service was modified after subscriptions existed, click **Update Subscriptions** to rebuild all user subscriptions. Subscriptions must be updated if the service URL was changed, a phone service parameter was removed, or the parameter name for a phone service parameter was changed.

Note

If the service URL was changed, remove a Cisco IP Phone Service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed. Be sure to click **Update Subscriptions** to update all currently subscribed users with the changes. If this is not done, users must resubscribe to the service to rebuild the URL correctly.

— If the service is new and you do not need to rebuild user subscriptions, click **Save**.

The table provides information about the Cisco IP Phone Services Configuration parameters.

Field	Description
Service Name	Enter the name of the service as it will display on the menu of available services in the Cisco Unified IP Phone User Options application. Enter up to 32 characters for the service name.
ASCII Service Name	Enter the name of the service to display if the phone cannot display Unicode.
Service Description	Enter a description of the content that the service provides.
Service URL	Enter the URL of the server where the Cisco IP Phone Services application is located. Make sure that this server remains independent of the servers in your Cisco Unified Communications Manager cluster. Do not specify a Cisco Unified Communications Manager server or any server that is associated with Cisco Unified Communications Manager (such as a TFTP server or directory database publisher server).

Configure Cisco IP Phone Services – Step 2: Phone Services

Access the Cisco Unified Communications Manager Administrator and choose **Device > Device Settings > Phone Services** to configure Cisco IP Phone Services.

Configure IP Phone Services Step 2: Phone Services

Device >Device Settings > Phone Services

IP Phone Service (1 - 3 of 3) Rows per Page 50

Find Phone where Service Name begins with

	Service Name
<input type="checkbox"/>	Group
<input type="checkbox"/>	Login
<input type="checkbox"/>	phonedir

- To add an IP phone service, click the **Add New** button.
- To update a service, click the name of the Cisco IP Phone Service that you want to update.

To add a new Cisco IP Phone Service, click **New**. To update an existing service, click on the name of the appropriate service.

Configure Cisco IP Phone Services – Step 3: Parameters

The table explains the Cisco IP Phone Services parameters.

Configure IP Phone Services Step 3:
Phone Services Parameters

Device > Device Settings > Phone Services > Login

Service Information

Service Name*	ASCII Service Name*
Login	Login
Service Description	Service URL*
Login	http://10.192.5.97:8080/emapp/EMAppServlet?device=

Service Parameter Information

Parameters	New
	Edit
	Delete

- Save Delete Update Subscriptions Add New

- Service Name – a (meaningful) name for the service
- ASCII Service Name – name for ASCII-only phone displays
- Service Description – what the service does
- Service URL – where the service can be found

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-47

To enable a service, the following settings need to be configured:

Field	Description
Service Name	Enter the name of the service as it will display on the menu of available services in the Cisco Unified IP Phone User Options application. Enter up to 32 characters for the service name.
ASCII Service Name	Enter the name of the service to display if the phone cannot display Unicode.
Service Description	Enter a description of the content that the service provides.
Service URL	Enter the URL of the server where the Cisco IP Phone Services application is located. Make sure that this server remains independent of the servers in your Cisco Unified Communications Manager cluster. Do not specify a Cisco Unified Communications Manager server or any server that is associated with Cisco Unified Communications Manager (such as a TFTP server or directory database publisher server).

In addition, parameters can be defined that are sent to the application server when the service is accessed. These parameters can be customized on a per-phone basis, but it is also possible to define default values for every parameter. Examples for such parameters are user PINs and passwords.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- The Cisco Unified Communications Manager provides several predefined user features.
- Users can also use the BLF to speed dial a Directed Call Park number.
- The default Hold Reversion timeout is defined in the Cisco Communications Manager Service parameters and is overruled by a setting on the line.
- Users can use an intercom line only to dial other intercom lines.
- Barge uses built-in conference bridge; cBarge uses shared conference bridge.
- The User Options web page enables users to change the Call Forward Busy and No answer for assigned phones.
- The Cisco IP Phone Services menu is delivered by the Cisco Unified Communications Manager while the service itself comes from an application server.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-48

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager Features and Services Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfeat/fsgd.pdf
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Cisco Unified Communications Manager System Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmsys/accm.pdf

Lesson 3

Configuring Cisco Unified Presence-Enabled Speed Dials and Lists

Overview

Today, users are mobile, working from homes, in the office, in airport lounges, or while traveling. In order to be able to communicate with others efficiently, it is helpful to know about their current availability. Can they be reached by phone, by instant messaging, or e-mail, and are they ready to communicate at this point in time? Cisco Unified Communications solutions offer presence information about the reachability and status of a user.

Cisco Unified Communications Manager Presence, an integrated part of Cisco Unified Communications Manager, allows IP phone users to monitor the status of directory numbers. This lesson describes how Cisco Unified Communications Manager Presence works and how it is configured.

Objectives

Upon completing this lesson, you will be able to describe and configure Cisco Unified Presence-enabled speed dials and lists. This ability includes being able to meet these objectives:

- Introduce the Cisco Unified Presence feature, which is part of Cisco Unified Communications Manager
- Describe how Cisco Unified Communications Manager natively supports Cisco Unified Presence
- Describe how to configure Cisco Unified Presence in Cisco Unified Communications Manager
- Describe how access control for Cisco Unified Presence subscription is supported by Cisco Unified Communications Manager
- Describe how to configure Cisco Unified Presence access control in Cisco Unified Communications Manager

Cisco Unified Presence Essentials

This topic describes the essentials of Cisco Unified Communications Manager Presence.

Cisco Unified Presence Solutions

Multiple options to integrate presence:

- Cisco Unified Communications Manager Presence
 - Speed-dial presence
 - Call history presence
 - Presence policy
- Cisco Unified Presence Server
 - User status information
 - Cisco IP Phone Messenger application
 - Cisco Unified Personal Communicator
 - Third-Party Presence Server Integration

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-4

Cisco Unified Communications includes multiple options to integrate presence information. Cisco Unified Communications Manager Presence, a native presence feature of Cisco Unified Communications Manager, includes the following capabilities:

- **Presence-enabled speed dials:** Speed-dial buttons that indicate the status of the target of the speed dial.
- **Presence-enabled call and directory lists:** Call lists and directory entries that indicate the status of each list entry.
- **Presence policy:** Tools allowing access control to presence information.

When you use Cisco Unified Presence, many features are added to those provided by the native Cisco Unified Communications Manager Presence feature, including:

- Standards-based session initiation protocol (SIP) and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) network interface
- User status information, not only device (line) status information
- Instant messaging capabilities, including integration with third-party servers
- Cisco Unified Personal Communicator: A client tool that integrates voice, video, and instant messaging communications

Note This lesson covers Cisco Unified Communications Manager Presence only.

Cisco Unified Communications Manager Presence Characteristics

This subtopic describes the characteristics of Cisco Unified Communications Manager Presence.

Cisco Unified Communications Manager Presence Characteristics

- Natively supported by Cisco Unified Communications Manager
- Allows an interested party (a watcher) to monitor the real-time status of a directory number (a presence entity)
- Watcher **subscribes** to status information of the presence entity
- Watcher can show the status of a presence entity using:
 - Presence-enabled speed dials
 - Presence-enabled lists (call and directory lists)
- Three possible states of watched directory number:
 - Entity is unregistered
 - Entity is registered—on-hook
 - Entity is registered—off-hook

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-5

Cisco Unified Communications Manager Presence is natively supported by Cisco Unified Communications Manager, and no extra products or servers are required. It allows an interested party, the watcher or subscriber, to monitor the real-time status of a directory number, a presence entity, or “subscribee.”

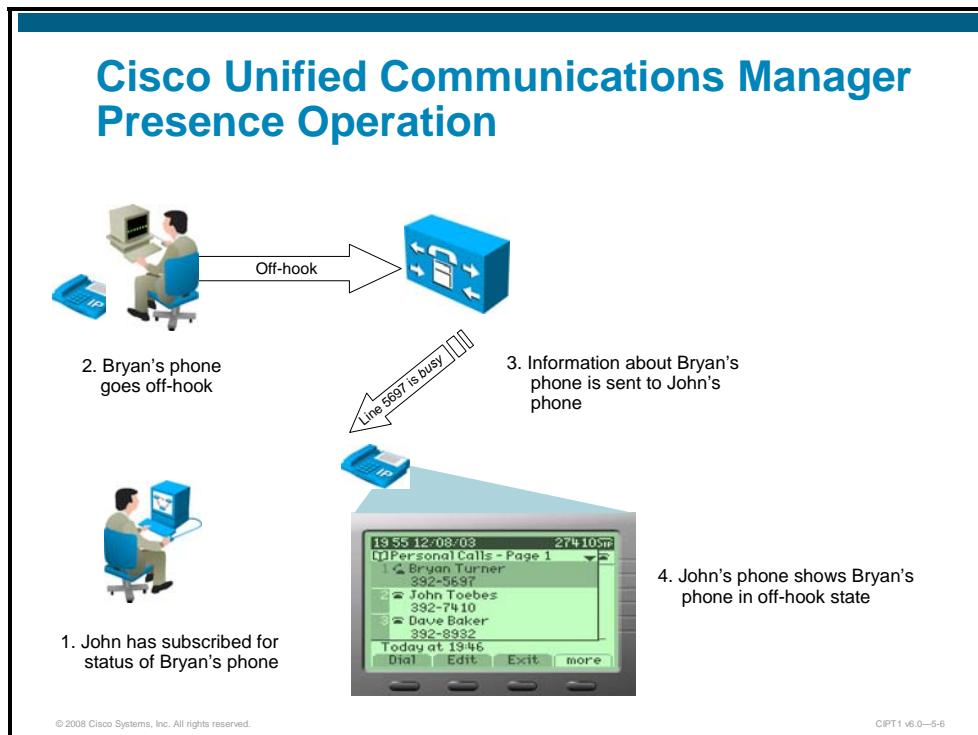
A watcher subscribes to the status information of one or more presence entities. The status information of a presence entity can be viewed using presence-enabled speed dials or presence-enabled lists—call lists such as placed, received, or missed calls and public directory lists.

The status can be one of the following:

- Unknown: This status is shown when the watched device is unregistered.
- On-hook
- Off-hook

Cisco Unified Communications Manager Presence Operation

The figure shows an example of the operation of Cisco Unified Presence.



In the example, John's phone subscribes to the status of Bryan's phone (more precisely, to the status of Bryan's directory number). John's phone is doing that because the Cisco Unified Communications Manager Administrator configured a presence-enabled speed dial for Bryan's extension, or because John is browsing through a call list that includes Bryan's directory number. John's phone also subscribes to the status of the other entries of the call list; this is done automatically as soon as the call list is viewed.

Cisco Unified Communications Manager Presence will now keep John's phone updated about the status of the subscribed presence entity, which means, if Bryan goes off-hook while John is browsing the call list that includes Bryan's directory number, the status information is displayed.

If John had a presence-enabled speed dial for Bryan's directory number, the speed dial would permanently display the current status of Bryan's directory number.

Cisco Unified Presence Support in Cisco Unified Communications Manager

This topic describes how Cisco Unified Communications Manager supports presence with the Cisco Unified Communications Manager Presence feature.

Cisco Unified Communications Manager Support for Presence

- Directory numbers (lines) of Cisco IP phones can be watched
 - By Cisco IP phones
 - By SIP devices through a SIP trunk
- Directory numbers (lines) of Cisco IP phones, and endpoints that are reached via SIP trunks, can be watched by the following:
 - Cisco IP phones
 - SIP devices through a SIP trunk

© 2008 Cisco Systems, Inc. All rights reserved.

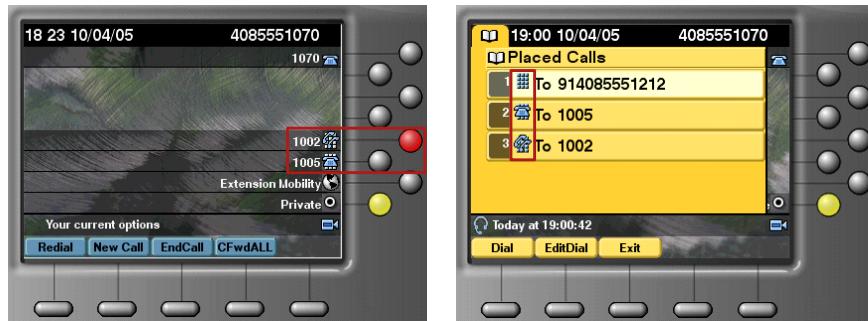
CIPT1 v6.0—5-8

Cisco Unified Communications Manager Presence allows directory numbers to be watched by Cisco IP phones and by SIP devices through a SIP trunk. Endpoints that can be reached through a SIP trunk can be watched by Cisco IP phones and by SIP devices through other trunks. Both Cisco IP phones running Skinny Client Control Protocol (SCCP) and Cisco IP phones running SIP can watch presence entities and can be watched. If presence subscriptions are sent over a SIP trunk, Cisco Unified Communications Manager takes care about protocol conversion between SCCP and SIP. If only IP phones that are registered within the Cisco Unified Communications Manager cluster are involved, there is no need for endpoint-to-endpoint communication because Cisco Unified Communications Manager is aware of the state of all registered IP phones.

Watching Presence Status on Cisco IP Phones

This subtopic describes how presence information can be watched on a Cisco IP phone.

Watching Presence Status on Cisco IP Phones



Presence status can be seen on speed-dial buttons, call lists and directories.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-9

Cisco IP phones can display status information (unknown, on-hook, or off-hook) of presence entities by presence-enabled speed dials or call and directory list entries.

Presence-enabled speed dials show a symbol in the screen of the IP phone, located at the appropriate speed dial button. Some phone models (type B Cisco Unified IP phones) have an LED inside the speed dial button and indicate the status by red (off-hook) or green (on-hook) lights.

When browsing through a directory or call list, each entry displays a symbol indicating its current status.

Cisco IP Phones That Support Viewing Presence Status

The table shows which type of status information is supported on Cisco IP phone models.

Cisco IP Phones That Support Viewing Presence Status

Cisco Unified IP Phone Models	Presence-Enabled Speed Dials Support	Presence-Enabled Call and Directory Lists Support
794[125], 796[125], 797[015] SIP and SCCP	Yes	Yes
7914, 7940, 7960 SCCP	Yes	No
7914, 7940, 7960 SIP	No	No

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-10

As shown in the table, Cisco Unified IP Phone 7914, 7940, and 7960 do not support presence at all when running SIP; when running SCCP, they support only presence-enabled speed dials but no presence-enabled call and directory lists. Type B Cisco Unified IP Phone 794[125], 796[125], and 797[015] support both presence-enabled call and directory lists and presence-enabled speed dials, regardless of the protocol (SIP or SCCP).

Note Cisco IP Communicator also supports both presence-enabled speed dials and presence-enabled call and directory lists.

Cisco Unified Presence Configuration

This topic describes how to configure Cisco Unified Communications Manager Presence.

Cisco Unified Communications Manager Presence Configuration Procedure

To enable presence-enabled speed dials:

1. Customize phone button templates to include presence-enabled speed-dial buttons
2. Apply phone button templates to phones
3. Configure presence-enabled speed-dial buttons
4. Apply subscribe CSS to phones

To enable presence-enabled call lists:

- Enable the **BLF For Call Lists** enterprise parameter

To allow presence subscriptions through SIP trunks:

- Enable Cisco Unified Communications Manager Presence on SIP trunks

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-12

The Cisco Unified Communications Manager Presence configuration procedure includes the following three parts:

■ **Enabling presence-enabled speed dials:**

- Step 1** Customize phone button templates to include presence-enabled speed-dial buttons.
- Step 2** Apply phone button templates to phones.
- Step 3** Configure presence-enabled speed-dial buttons.
- Step 4** Apply subscribe Calling Search Space (CSS) to phones.

Caution If partitions are used, so-called subscribe CSSs are required for subscriptions to succeed when trying to watch an entity that has a partition assigned.

■ **Enabling presence-enabled call lists:** Enable the BLF For Call Lists enterprise parameter.

Note In Cisco Unified Communications Manager configuration, presence-enabled call lists are referred to as busy lamp field (BLF) call lists.

■ **Allowing presence subscriptions through SIP trunks:** Enable Cisco Unified Communications Manager Presence on SIP trunks.

Note The first two features are independent of each other. The third feature is an optional add-on to both presence-enabled speed dials and presence-enabled call lists (if used).

Step 1: Customizing Phone Button Templates

This subtopic shows how to implement presence-enabled speed dials. The first step is the configuration of a phone button template as shown in the figure.

Step 1: Customizing Phone Button Templates

Device > Device Settings > Phone Button Template

Phone Button Template Configuration

Phone Button Template Information

Button Template Name * 7961 SCCP with 2 BLF-SD

Button Information

Button	Feature	Label
1	Line **	Line
2	Line	Line
3	Speed Dial	Speed Dial1
4	Speed Dial	Speed Dial2
5	Speed Dial BLF	Speed Dial BLF1
6	Speed Dial BLF	Speed Dial BLF2
7	None	
8	None	

Configure presence-enabled speed-dial buttons in phone button template

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-13

The first step for implementing presence-enabled speed dials is to configure a phone button template that includes presence-enabled speed dials. To configure a phone button template, go to **Device > Device Settings > Phone Button Template** and either add a new template or copy one of the default phone button templates and save it with a new name. Configure the phone button template with the desired number of presence-enabled speed dials.

Note In Cisco Unified Communications Manager Administration, presence-enabled speed dials are called speed-dial BLF.

Step 2: Applying the Phone Button Template to IP Phones

The figure shows how a phone button template is applied to an IP phone.

Step 2: Applying the Phone Button Template to IP Phones

Device > Phone

Phone Configuration

Phone Type

Product Type: Cisco 7960
Device Protocol: SCCP

Device Information

Registration	Registered with Cisco Unified Communications Manager 10.1.1.1 10.1.1.24
IP Address	001201545D98
MAC Address*	
Description	Phone1
Device Pool*	Default
Common Device Configuration	< None >
Phone Button Template*	7960 SCCP with 2 BLF-SD
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile

Assign phone button template to phone

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-14

Assign the previously configured phone button template to the IP phone that should be configured for presence-enabled speed dials. Go to the phone configuration page and select the appropriate template from the Phone Button Template drop-down list.

Step 3: Configuring Cisco Unified Presence-Enabled Speed-Dial Buttons

The figure shows the configuration of a presence-enabled speed-dial button.

Step 3: Configuring Presence-Enabled Speed Dial Buttons

Device > Phone

Phone Configuration

Association Information

Modify Button Items					
1	Line [1] - Add a new DN				
2	Line [2] - Add a new DN				
3	Add a new SD				
4	Add a new SD				
5	Add a new BLF SD				
6	Add a new BLF SD				

At the phone configuration page, click links to add a presence-enabled speed dial.

Add a new BLF SD

Enter presence-enabled speed-dial configuration: presence entity to watch and label to be displayed on phone

Busy Lamp Field Speeddial Configuration SEP001201545D98

Busy Lamp Field/Speed Dial Button Settings

Destination	Directory Number	Label	Label ASCII
1	1002	< None >	Phone2
2	1003	< None >	Phone3

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-15

After applying the new phone button template, the presence-enabled speed dials are displayed in the Association Information area of the phone configuration window. The phone now has the capability to use buttons for presence-enabled speed dials, but in order to use the buttons that way, the buttons have to be configured appropriately. To configure presence-enabled speed dials, click on the **Add a new BLF-SD** link. The Busy Lamp Field Speeddial Configuration window appears. In this window configure the target (the presence entity to be watched) of the presence-enabled speed-dial button and a label which will be displayed on the phone screen next to the corresponding button.

Note	In Cisco Unified Communications Manager configuration, presence-enabled speed dials are referred to as BLF speed dials.
-------------	---

Enabling Cisco Unified Presence-Enabled Call Lists

This subtopic shows how to enable presence-enabled call lists.

Enabling Presence-Enabled Call Lists

System > Enterprise Parameters

Enterprise Parameters Configuration

Parameter Name	Parameter Value	Suggested Value
Synchronization_Between_Auto_Device_Profile_and_Phone_Configuration *	True	True
Max_Number_of_Device_Level_Trace *	12	12
DSCP_for_Phone-based_Services *	default DSCP (000000)	CP
DSCP_for_Phone_Configuration *	CS3(precedence 3) DSCP (011000)	CP
DSCP_for_Cisco_CallManager_to_Device_Interface *	CS3(precedence 3) DSCP (011000)	
Connection_Monitor_Duration *	120	120
Auto_Registration_Phone_Protocol *	SCCP	SCCP
BLF_For_Call_Lists *	Enabled	Disabled
Advertise_G.722_Codec *	Enabled	Enabled
Phone_Personalization *	0	0

If call lists should also provide presence information, the appropriate enterprise parameter has to be enabled, as shown in the figure. After changing the BLF For Call Lists enterprise parameter to Enabled, all phones that support presence-enabled call lists must be reset in order for the change to become effective

Note In Cisco Unified Communications Manager configuration, presence-enabled call lists are referred to as BLF call lists.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-16

Enabling Cisco Unified Presence on SIP Trunks

This subtopic shows how to allow presence subscriptions over SIP trunks.

The screenshot shows the Cisco Unified Presence interface. On the left, under 'System > Security Profile > SIP Trunk Security Profile Configuration', there is a form for 'SIP Trunk Security Profile Information'. It includes fields for Name (Non Secure Presence Enabled SIP Trunk Profile), Description (Non Secure SIP Trunk Profile with Presence Enabled), Device Security Mode (Non Secure), Incoming Transport Type (TCP+UDP), Outgoing Transport Type (TCP), and several checkboxes for authentication and presence handling. A red box highlights the 'Accept Presence Subscription' checkbox. In the center, under 'Trunk Configuration > SIP Information', there is another form where the 'SIP Trunk Security Profile' dropdown is set to 'Non Secure Presence Enabled SIP Trunk Profile'. A red box highlights this selection. To the right, a separate window titled 'Assign SIP Trunk Security Profile to SIP Trunk' shows a dropdown menu with the same profile selected. A red box highlights this selection. A callout box labeled 'Configure SIP Trunk Security Profile for presence' points to the 'Accept Presence Subscription' checkbox in the main configuration window. Another callout box labeled 'Assign SIP Trunk Security Profile to SIP Trunk' points to the selected profile in the assign window. The bottom of the interface has copyright information and a page number (CIPT1 v6.0—5-17).

If presence subscriptions are possible over a SIP trunk, presence needs to be enabled on the SIP trunk. Presence is not enabled directly at the SIP trunk but via a SIP Trunk Security Profile. Therefore configure a SIP trunk security profile from **System > Security Profile > SIP Trunk Security Profile**, where the Accept Presence Subscriptions and the Accept Unsolicited Notification check boxes are activated. Then apply the SIP trunk security profile to the SIP trunk, as shown in the figure.

Cisco Unified Presence Policies

This topic describes how to implement Cisco Unified Presence policies in order to control which presence entities can be monitored by which watcher.

Limiting Presence Visibility

Cisco Unified Communications Manager Presence offers different ways to limit visibility of presence information:

- Presence-enabled speed dials
 - Are **statically configured** by Cisco Unified Communications Manager Administrator (cannot be configured by users)
 - **Subscribe Calling Search Space** and (standard) partitions
- Presence-enabled call and directory lists
 - **Subscribe Calling Search Space** and (standard) partitions
 - Presence groups

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-19

Cisco Unified Communications Manager Presence can limit visibility of presence information in the following ways:

- Presence-enabled speed dials are configured statically by the Cisco Unified Communications Manager administrator and cannot be configured or modified by a user. In this way, the administrator has control over the monitored presence entities for each individual watcher. However, partitions and subscribe calling search spaces also apply to presence-enabled speed dials.
- Access control for presence-enabled call and directory lists can be provided by partitions and subscribe calling search spaces and by presence groups. Each of the two methods can be used independently of each other. If both are used, both have to permit a subscription for successful watching of the presence entity status.

Subscribe CSS and Partitions

This subtopic describes how to use subscribe CSS and partitions to implement presence policies.

Subscribe CSS and Partitions

- Separate CSSs are applied for calling privileges and presence: the (standard) CSS for calling privileges and a subscribe CSS for presence.
- A subscribe CSS is applied to a watcher: a SIP trunk, a phone, or an end user.
- The subscribe CSS determines which presence entities a watcher is allowed to monitor.
- Similar to with traditional CSSs, a presence entity can only be watched if the watcher has the presence entity's partition in its subscribe calling search space.
- The (standard) partition that is applied to a line or a route pattern referring to a trunk is used for both calling privileges and presence.
- If no partition is applied to a line or route pattern, it is available to all watchers.

© 2008 Cisco Systems, Inc. All rights reserved.

CPT1 v6.0—5-20

Calling privileges are implemented using partitions and CSSs. Presence policies are implemented by using the *same* partitions (applied to directory numbers and route patterns) that are used for calling privilege configuration; the CSSs, however, are separated. Rather than the (standard) CSS configured on IP phones, lines, and trunks, dedicated subscribe CSSs are used.

A subscribe CSS is applied to a watcher. This can be a SIP trunk (assuming that subscriptions have been enabled in general on the trunk), a phone, or an end user. Subscribe CSSs do not use the concept of a device CSS and a line CSS. Watching a presence entity is always a global function of the IP phone, not of a certain line. Therefore, subscribe CSSs are only applied to IP phones and not to lines. When a subscribe CSS is applied to an end user, this subscribe CSS is used in case of extension mobility or if the end user is associated with a device.

Similar to standard CSSs, the subscribe CSS determines which presence entities a watcher is allowed to monitor. A subscription is only permitted if the watcher has the partition of the desired presence entity in its subscribe CSS.

The (standard) partition which is applied to a line or a route pattern that refers to a SIP trunk is used for both calling privileges and presence policies. If no partition is applied to the desired presence entity, the presence entity is available to all watchers.

Subscribe CSS and Partition Considerations

This subtopic describes what needs to be considered when implementing calling privileges or presence policies using partitions.

Subscribe CSS and Partition Considerations

- Presence policies and calling privileges share some configuration settings:
 - Partitions on lines and route patterns
- Implementing presence policies impacts calling privileges and vice versa
 - Any changes to **partition** configuration affects calling privileges (standard CSSs) and presence policies (subscribe CSSs)
- **Design and implementation of calling privileges and presence policies have to be performed together!**

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-21

Presence policies and calling privileges share a configuration element. The partitions that are applied to lines or route patterns apply to both. Therefore implementing presence policies impacts existing calling privileges, and vice versa.

Whenever partition configuration is changed because of the implementation of one of the two features (calling privileges and presence policies), the other feature is affected. Therefore, calling privileges and presence policies have to be designed and implemented together.

Subscribe CSS and Partition Considerations: Sample Scenario

This subtopic provides a sample scenario illustrating the dependencies of calling privilege implementation and presence policies implementation.

Subscribe CSS and Partition Considerations – Sample Scenario

- Baseline configuration does not include any partitions (no calling privileges and no presence policies are in place).
- If partitions and (standard) CSSs are implemented for calling privileges, subscriptions will fail:
 - Lines and route patterns now have partitions.
 - Devices (phones and trunks) do not have subscribe CSSs
- If partitions and subscribe calling search spaces are implemented for presence policies, calls will fail:
 - Lines and route patterns now have partitions.
 - Devices (phones, lines, and trunks) do not have CSSs.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-22

In the example scenario, the baseline configuration does not include any partitions and calling search spaces. Neither calling privileges nor presence policies are in place. All directory numbers and route patterns are in the null partition and can be accessed by all devices. All devices can place calls to all destinations. Presence subscriptions are also possible to all supported targets such as directory numbers and devices reached through SIP trunks.

If calling privileges (partitions and CSS) are implemented without considering presence (also adding subscribe CSSs), presence subscriptions will not work anymore for all presence entities that have been put into partitions when implementing calling privileges.

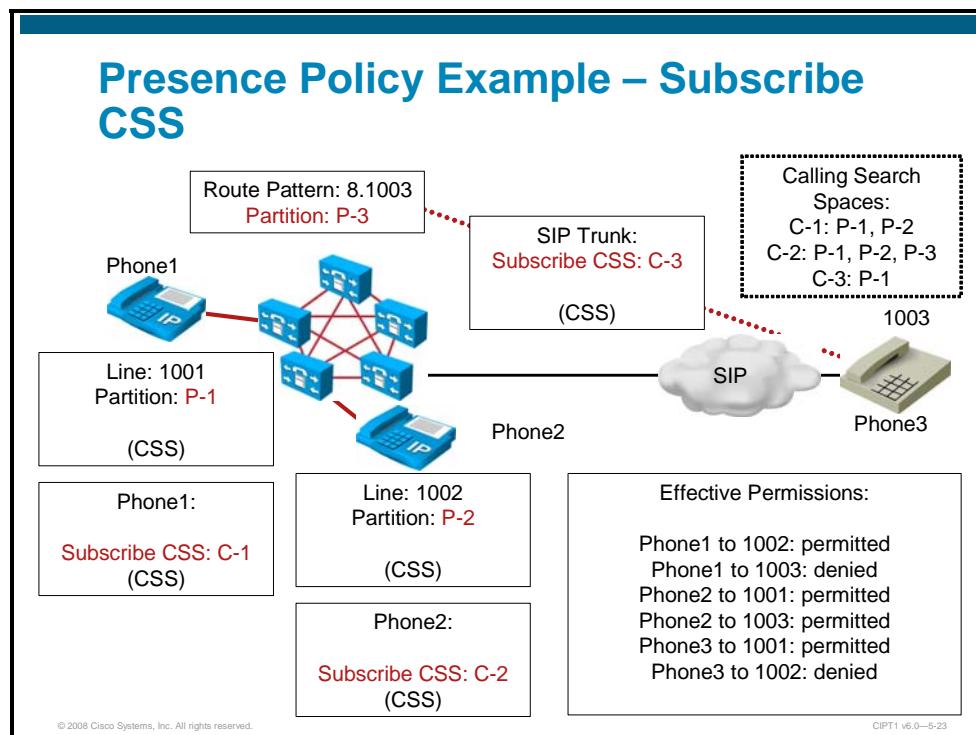
Note

The recommendation when implementing partitions and CSS is not to leave any targets in the null partition, but to assign a partition to all call destinations. Therefore, in the above scenario, usually there will be no targets left where subscriptions would still work.

Or, if the baseline configuration is modified in the way that presence policies (partitions and subscribe CSSs) are implemented, without considering calling privileges (also adding standard CSSs), all calls will fail. This will happen because lines and route patterns now have partitions but calling devices do not have CSSs that would allow access to some partitions. The devices only have subscribe CSSs, so only presence information can be obtained, but no calls can be placed.

Presence Policy Example: Subscribe CSS

The figure illustrates a presence policy example based on partitions and subscribe CSSs.



The configuration consists of three CSSs: C-1 contains partitions P-1 and P-2. C-2 contains partitions P-1, P-2, and P-3. C-3 contains partition P-1 only.

Phone1 has partition P-1 applied to its line, which is configured with directory number 1001. CSS C-1 is assigned to Phone1.

Phone2 has partition P-2 applied to its line, which is configured with directory number 1002. CSS C-2 is assigned to Phone2.

A SIP phone with number 1003 can be reached through a SIP trunk. The corresponding route pattern 8.1003 is in partition P-3. CSS C-3 is assigned to the SIP trunk.

The effective permissions for presence subscriptions are as follows:

Phone1 is allowed to watch the status of 1002 but not of 1003. Phone2 is allowed to watch both other phones. Phone 3 is allowed to subscribe to presence information of 1001 but not of 1002.

Note The "(CSS)" in the figure refers to the standard CSS used for the implementation of calling privileges. They are not relevant for the discussion of presence subscription permissions but because they also depend on the configured partitions, they are added to illustrate that they have to be considered in the overall configuration.

Note Partitions and subscribe CSSs apply to both presence features: presence-enabled speed dials and presence-enabled call lists.

Presence Groups

Presence policies can be implemented by partitions and subscribe CSSs, or by presence groups. This subtopic describes how presence policies are implemented using presence groups.

Presence Groups

Presence groups can be used to implement presence policies:

- Watchers and presence entities are put into presence groups.
- Subscriptions are permitted within presence groups.
- Subscriptions can be allowed or denied between presence groups.
 - Permission can be configured independently for each direction
- IP phones have separate presence groups.
 - Line presence group (presence entity)
 - Phone presence group (watcher)
- SIP trunks have only one presence group.
 - used for both watcher and presence entity
- **Presence groups only apply to presence-enabled call lists – they do not apply to presence-enabled speed dials**

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-24

When implementing presence policies, watchers and presence entities are put into presence groups. Subscriptions can be allowed or denied at an intergroup level; within a presence group, subscriptions are always permitted (unless denied by partitions and subscribe CSSs).

IP phones are configured with two or more presence groups. One presence group is applied to the device (in the role as a watcher), and each line can be configured with a presence group in its role as a presence entity.

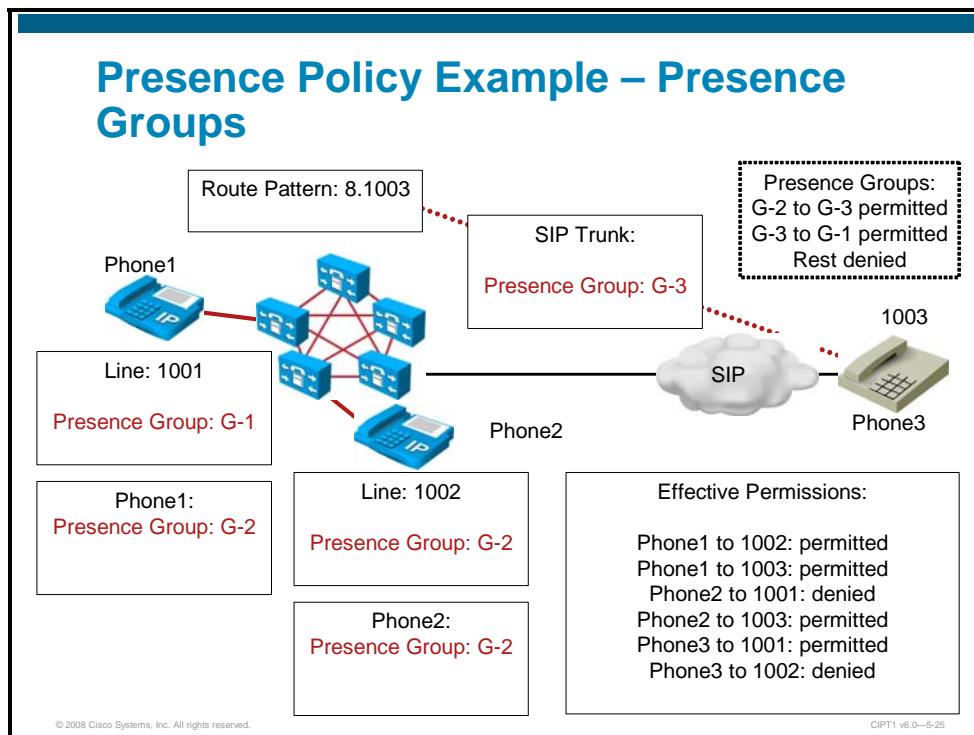
On SIP trunks, only one presence group is configured, which is used in both roles, as a watcher and as a presence entity. You cannot assign a presence group to a route pattern.

Like subscribe CSSs, presence groups can also be assigned to end users. They are used when the end users are logging into the phone using extension mobility or when the users are associated with a device.

Note	Presence groups only apply to presence-enabled call lists – they do not apply to presence-enabled speed dials.
-------------	--

Presence Policy Example: Presence Groups

The figure illustrates a presence policy example based on presence groups.



The configuration uses three presence groups: G-1, G-2, and G-3. Inter-presence group subscriptions are permitted from G-2 to G-3 and G-3 to G-1. All other inter-presence group subscriptions are denied.

Phone1 has presence group G-1 applied to its line, which is configured with directory number 1001. Presence group G-2 is assigned to Phone1.

Phone2 has presence group G-2 applied to its line, which is configured with directory number 1002. Presence group G-2 is also assigned to Phone2.

A SIP phone with number 1003 can be reached through a SIP trunk. Presence group G-3 is assigned to the SIP trunk.

The effective permissions for presence subscriptions are as follows:

Phone1 is allowed to watch the status of 1002 and 1003. Phone2 is allowed to watch 1003 but not 1001. Phone 3 is allowed to subscribe to presence information of 1001 but not of 1002.

Note Presence groups apply only to presence-enabled call lists. Presence-enabled speed dials are not affected by presence groups.

Interaction of Presence Groups, Partitions, and Subscribe CSSs

This subtopic describes the interaction of presence groups, subscribe CSSs, and partitions.

Interaction of Presence Groups and Partitions and Subscribe CSSs

Presence groups, partitions, and subscribe CSSs can be combined.

- Both have to permit subscription for successful watching
- Provides 2 levels of hierarchy – useful in larger deployments
- Example:
 - Requirements:
 - No subscriptions are allowed across departments.
 - Within a department, managers can only be watched by their assistants.
 - Solution:
 - Use one presence group per department.
 - Deny inter-presence group subscriptions.
 - Include manager partition only in the subscribe CSS of their assistant.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-26

Each feature can be used standalone or they can be combined. If both uses are implemented, both mechanisms have to permit the subscription in order to allow successful watching.

Combining both presence policy mechanisms provides two hierarchy levels, which is useful in larger deployments or complex scenarios.

The following example illustrates how subscribe CSSs and partitions and presence groups can be effectively combined to fulfill the given requirements:

Requirements: No subscriptions are allowed between different departments. Within a department, managers can only be watched by their assistants. All other subscriptions within a department should be possible.

Solution: One presence group is configured per department. Inter-presence group subscriptions are denied by setting the default inter-presence group policy accordingly. One partition is configured per manager. Each of these partitions is only listed in the subscribe CSS of the respective manager assistant.

In the example, presence groups are used for the first level of presence policies (at department level) and subscribe CSSs and partitions are used for additional access control within a department (or presence group).

Note

Presence groups only apply to presence-enabled call lists. They do not apply to presence-enabled speed dials.

Cisco Unified Presence Policy Configuration

This topic describes how to implement presence policies in Cisco Unified Communications Manager.

Unified CM Presence Policies Configuration Procedure

To implement presence policies based on partitions and CSSs:

1. Configure partitions and CSSs
2. Assign partitions to lines and route patterns
3. Assign subscribe CSSs to phones and trunks

To implement presence policies based on presence groups:

1. Configure presence groups
2. Set the default inter-presence group policy
3. Assign presence groups to lines, phones, and SIP trunks

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-28

The Cisco Unified Communications Manager presence policy configuration procedure includes the following parts:

- Implement presence policies based on partitions and CSSs:

Step 1 Configure partitions and CSSs

Step 2 Assign partitions to lines and route patterns

Step 3 Assign subscribe CSSs to phones and trunks

- Implement presence policies based on presence groups:

Step 1 Configure presence groups

Step 2 Set the default inter-presence group policy

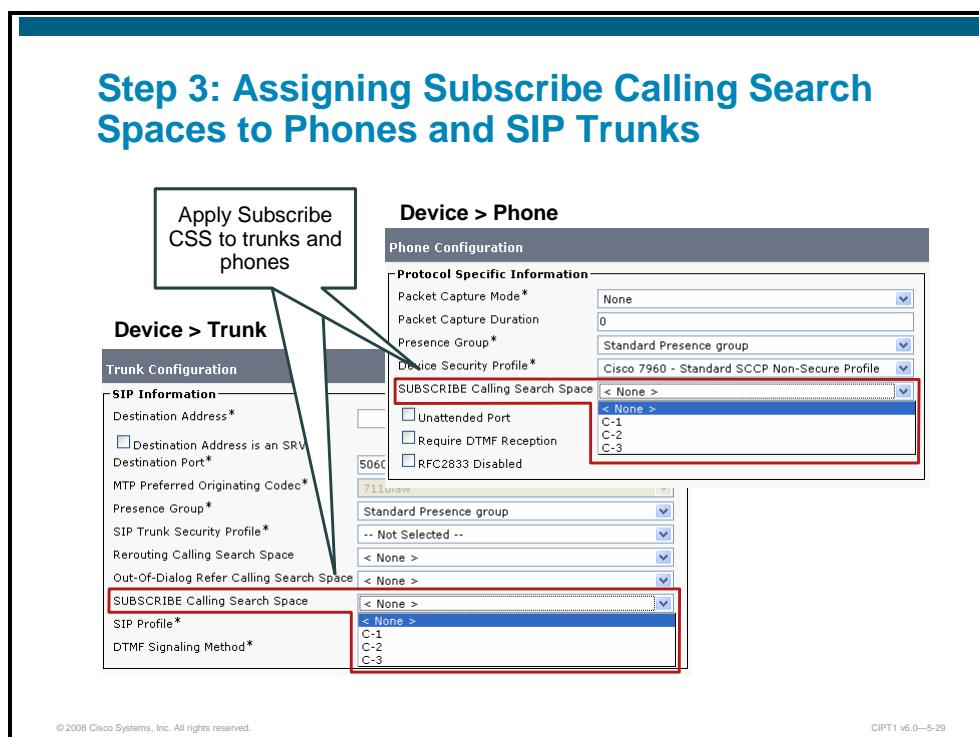
Step 3 Assign presence groups to lines, phones, and SIP trunks

Note These two procedures can be independently configured. Presence groups only apply to presence-enabled call lists and subscribe CSSs. Partitions apply to presence-enabled call lists and presence-enabled speed dials.

Implementing Presence Policies Based on Partitions and CSS:

Step 3 – Assigning Subscribe CSSs to Phones and SIP Trunks

The first two steps of implementing presence policies based on partitions and subscribe CSSs are not shown because they have been covered in earlier lessons of this course.

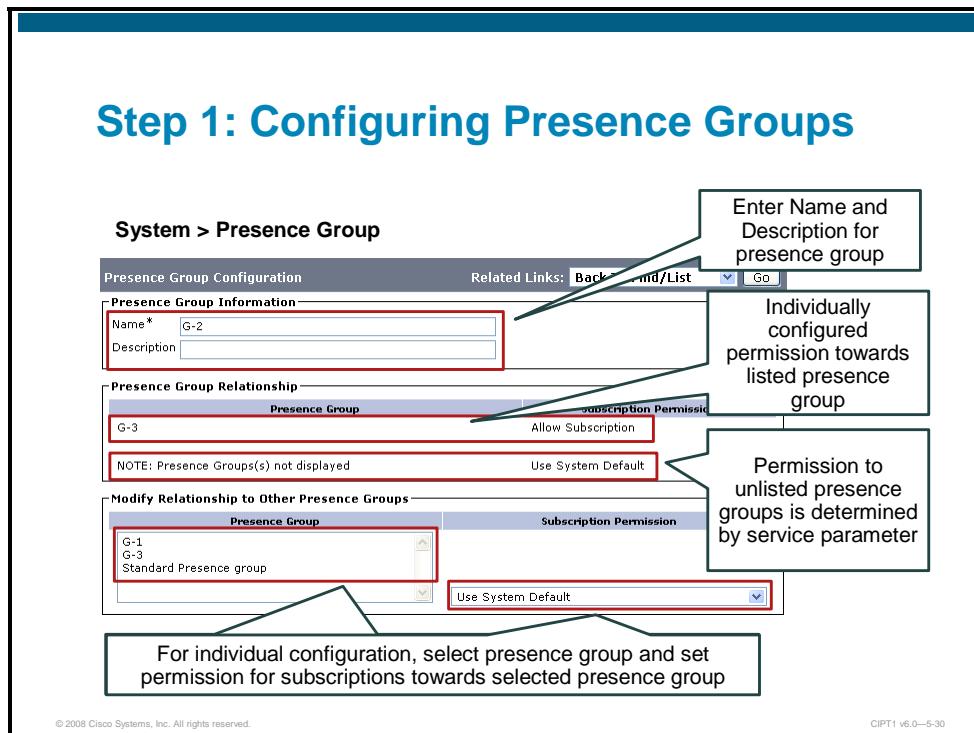


The figure shows how CSSs are assigned to IP phones and SIP trunks as SUBSCRIBE Calling Search Spaces.

Implementing Presence Policies Based on Presence Groups:

Step 1 – Configuring Presence Groups

This subtopic shows how to implement presence policies based on presence groups. Note that presence groups only apply to presence-enabled call lists and are ignored by presence-enabled speed dials. The first step when implementing presence groups is to add and configure presence groups, as shown in the figure.



Presence groups can be added and configured from **System > Presence Group**. One presence group exists by default and cannot be deleted; it is called Standard Presence group. All phones, lines, and SIP trunks, by default, are members of the Standard Presence group. The Standard Presence group can be modified in the way that the permissions to other groups can be set, but it cannot be deleted.

When adding a new presence group, enter a Name and Description and configure the permission for subscriptions toward other presence groups. The permission does not have to be entered toward all other presence groups; the permission for subscriptions towards unconfigured presence groups will be determined by system default, which is configurable as a Cisco CallManager service parameter.

Note	Subscription Permissions are configured in a <i>unidirectional</i> manner between pairs of presence groups. It is possible to permit subscriptions from one group to another but to deny subscriptions in the opposite direction.
-------------	---

Step 2: Setting the Default Inter-Presence Group Policy

The figure shows the configuration of the default inter-presence group policy.

Step 2: Setting the Default Inter-Presence Group Policy

System > Service Parameter (Cisco CallManager)

Clusterwide Parameters (System - Presence)

Presence Subscription Throttling Threshold.*	90000	90000
Presence Subscription Resume Threshold.*	80	80
Default Inter-Presence Group Subscription.*	Disallow Subscription	<input checked="" type="checkbox"/> Disallow Subscription

Set the Default Inter-Presence Group Subscription

The Default Inter-Presence Group Subscription specifies the system default for presence subscriptions towards presence groups for which no explicit permission has been configured.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-31

The Default Inter-Presence Group Subscription service parameter specifies the system default for presence subscriptions. The system default is applied for subscriptions toward presence groups for which no explicit permission has been set in the configuration of the presence group from which the subscription request has been sourced.

The Default Inter-Presence Group Subscription parameter is a service parameter of the Cisco CallManager service and is therefore configured from **System > Service Parameter**.

Step 3a: Assigning Presence Groups to Lines and Phones

The figure shows how a presence group is applied to lines and phones.

Step 3a: Assigning Presence Groups to Lines and Phones

Device > Phone

Phone Configuration

Protocol Specific Information

Packet Capture Mode*: None

Packet Capture Duration: 0

Presence Group*: Standard Presence group (highlighted)

Device Security Profile*: Standard Presence group (highlighted)

SUBSCRIBE Calling Search Space: G-1, G-2, G-3

Unattended Port

Require DTMF Reception

RFC2833 Disabled

Assign presence group to phone (in subscriber role)

Call Routing > Directory Number

Directory Number Configuration

Directory Number Settings

Voice Mail Profile: < None >

Calling Search Space: < None >

Presence Group*: Standard Presence group (highlighted)

User Hold MOH Audio Source: Standard Presence group (highlighted)

Network Hold MOH Audio Source: G-1, G-2, G-3

Auto Answer*: Auto Answer Off

© 2008 Cisco Systems, Inc. All rights reserved.CIPT1 v6.0—5-32

Presence groups allow the implementation of presence policies by checking the permission for subscriptions going from one presence group to another presence group. This means that each subscriber and each presence entity must be in a presence group.

IP phones (and their lines) act as both: the IP phone itself generates subscriptions (when using presence-enabled speed dials or presence-enabled call lists) and their directory numbers can be watched by other subscribers. Therefore, presence groups are applied to both: the phone (in the role as a subscriber) and all phone lines (in the role as a presence entity).

Note By default, all phones and all lines are in the Standard Presence group.

Note Remember that presence groups apply to presence-enabled call lists only. Therefore, subscriptions caused by presence-enabled speed dials are ignoring all presence group-based policies.

Step 3b: Assigning a Presence Group to a SIP Trunk

The figure shows how a presence group is applied to a SIP trunk.

Step 3b: Assigning a Presence Group to a SIP Trunk

Device > Trunk

Trunk Configuration

SIP Information

Destination Address*: [Input Field]

Destination Address is an SRV

Destination Port*: 5060

MTP Preferred Originating Codec*: 7110law

Presence Group* [Red Box]

SIP Trunk Security Profile*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile*

DTMF Signaling Method*

A dropdown menu for "Presence Group" is open, showing:

- Standard Presence group
- Standard Presence group (highlighted)
- G-1
- G-2
- G-3

Annotations:

- A callout points to the "Presence Group" dropdown with the text: "Assign presence group to SIP trunk".
- A callout points to the "Standard Presence group" option in the dropdown with the text: "Same presence group is used in subscriber and presence entity role".

The presence group configured on a SIP trunk applies to both subscriptions being sent out and being received on the trunk.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-33

Cisco Unified Communications Manager can send subscribe messages out on a SIP trunk (when watching a presence entity located on the other side of the trunk) and can receive subscriptions on a SIP trunk (when a local directory number is watched over the SIP trunk by a subscriber located on the other side of the trunk). The trunk, therefore, can act in both subscriber and presence entity roles. However, on a SIP trunk, only one presence group can be configured and therefore this single presence group applies to sent subscriptions as well as to received subscriptions.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco Unified Communications Manager Presence allows lines or endpoints reachable through SIP trunks to be monitored for their status (on-hook versus off-hook).
- Most IP phones support presence-enabled speed dials; type B Cisco IP phones using SIP also support presence-enabled call and directory lists.
- Cisco Unified Communications Manager Presence configuration includes implementing presence-enabled speed dials and enabling presence-enabled call and directory lists.
- Cisco Unified Presence policies can be applied for controlling presence subscriptions.
- Cisco Unified Communications Manager Presence policy configuration includes implementing partitions and subscribe calling spaces and presence groups.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-34

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager Features and Services Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfeat/fsgd.pdf
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html

Lesson 4

Integrating Cisco Unified Communications Manager with Voice-Mail Systems

Overview

This lesson describes integrating Cisco Unity with Cisco Unified Communications Manager, Cisco Unity initial setup, and configuring a few voice-mail accounts.

Objectives

Upon completing this lesson, you will be able to integrate Cisco Unified Communications Manager with voice-mail systems and set up basic voice-mail functionality. This ability includes being able to meet these objectives:

- Describe Cisco Unified Communications Manager voice-mail integration
- Describe Cisco Unity
- Describe Cisco Unified Communications Manager Configuration for voice-mail integration
- Describe Cisco Unified Communications Manager phone configuration for voice-mail usage
- Describe Cisco Unity Configuration for Cisco Unified Communications Manager integration
- Configure Cisco Unity Subscriber

Cisco Unified Communications Manager Voice-Mail Integration Essentials

This topic describes Cisco Unified Communications Manager voice-mail integration and provides an overview of the components.

Cisco Unified CM Voice-Mail Integration

- Cisco Unified CM can integrate with Cisco Unity, Cisco Unity Connection, Cisco Unity Express.
- Cisco Unity and Cisco Unity Connection integrate using SIP or SCCP:
 - SIP integrations include MWI handling.
 - SCCP needs additional MWI ports.
- Cisco Unity can handle multiple clusters connected through QSIG tunnels.
- Cisco Unity uses the forwarding information provided by Unified CM to answer the call appropriately.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-4

Cisco Unified Communications Manager can integrate with Cisco Unity and Cisco Unity Connection via either Skinny Client Control Protocol (SCCP) or session initiation protocol (SIP).

Cisco Unity telephony integrations are configured with the Cisco Unity Telephony Integration Manager (Cisco UTIM), while Cisco Unity Connection is configured using the System Administrator GUI.

In addition to the option of adding multiple clusters by adding additional integrations for each new Cisco Unified Communications Manager cluster in Cisco Unity, Cisco Unified Communications Manager supports Annex M.1, Message Tunneling for Q Signaling (QSIG), which gives administrators the ability to enable QSIG on intercluster trunks (ICTs) between Cisco Unified Communications Manager clusters.

The phone system sends the following information with forwarded calls to the voice-mail system:

- The extension of the called party
- The extension of the calling party (for internal calls) or the phone number of the calling party (if it is an external call and the system uses caller ID)
- The reason for the forward (the extension is busy, does not answer, or is set to forward all calls)

Cisco Unity uses this information to answer the call appropriately. For example, a call forwarded to Cisco Unity is answered with the personal greeting of the subscriber. If the phone system routes the call without this information, Cisco Unity answers with the opening greeting.

Third-Party Voice-Mail Systems

This subtopic describes third-party voice-mail systems.

Third-Party Voice-Mail Systems

- Using SMDI Interface over analog lines, the Cisco Unified CM supports:
 - Octel 100, 200/300, and 250/350
 - Intuity Audix
 - Siemens PhoneMail
 - Centigram/BayPoint (OnePoint and NuPoint Messenger)
 - Lyrix ECS
 - IBM Message Center
- Using the SMDI of the VG248, it is possible to integrate:
 - NEC Message Center Interface (MCI)
 - Ericsson MD110

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-5

The Cisco Messaging Interface is a Cisco CallManager service that should run only on the publisher server.

This service intercepts calls destined for voice-mail and generates appropriate Simplified Message Desk Interface (SMDI) messages, which are then delivered to one of the server Component Object Model (COM) ports. The Cisco Messaging Interface service is compatible with any Media Gateway Control Protocol (MGCP) gateway that supports analog Foreign Exchange Station (FXS) ports or T1 channel associated signaling (CAS) recEive and transMit, or ear and mouth (E&M); however, the Cisco Catalyst 6000 WS-X6624-FXS and Cisco VG224 Voice Gateway modules are two of only three gateways that support positive disconnect supervision and are therefore the only gateways currently recommended for use with the Cisco Messaging Interface service.

Through the Cisco Messaging Interface, Cisco Unified Communications Manager supports integration with virtually any voice-mail system that can provide SMDI with analog FXS ports, including (but not limited to) the following:

- Octel 100, 200/300, and 250/350
- Intuity Audix
- Siemens PhoneMail
- Centigram/BayPoint (OnePoint and NuPoint Messenger)
- Lyrix ECS
- IBM Message Center

The Cisco VG248 is an SCCP gateway that supports 48 analog FXS ports and generates SMDI locally (that is, it runs independent of the Cisco Messaging Interface service). As with the Cisco

WS-X6624 and Cisco VG224 modules, the Cisco VG248 also supports positive disconnect supervision.

Voice-mail integration through the Cisco VG248 provides the following features and advantages:

- Multiple SMDI links per Cisco Unified Communications Manager
- SMDI failover capability
- Independence from the location of the voice-mail system

The Cisco VG248 is also capable of supporting two other serial protocols that are sometimes used for voice-mail integration: NEC MCI and Ericsson MD110 proprietary protocols.

Cisco Unified Communications Manager and Cisco Unity Integration Using SCCP

Cisco Unity and Cisco Unified Communications Manager can integrate using SCCP or SIP. This topic describes the features of an integration using SCCP.

Features of Unified CM and Cisco Unity Integration using SCCP

The Cisco Unified CM SCCP integration with Cisco Unity provides the following features:

- Call Forward to personal greeting
- Call Forward to busy greeting
- Caller ID
- Easy message access (retrieve messages without entering an ID)
- Identified subscriber messaging (Cisco Unity automatically identifies internal subscriber based on the extension)
- Message Waiting Indicator (MWI)

© 2008 Cisco Systems, Inc. All rights reserved.

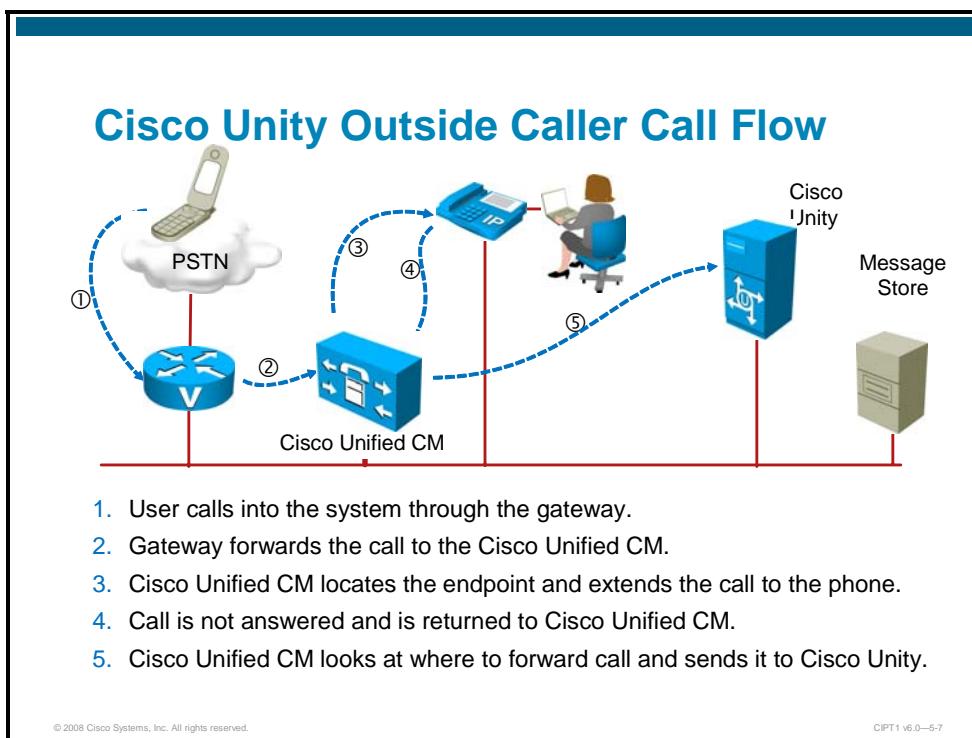
CIPT1 v6.0—5-6

The Cisco Unified Communications Manager SCCP integration with Cisco Unity provides the following features:

- Call Forward to personal greeting
- Call Forward to busy greeting
- Caller ID
- Easy message access (A subscriber can retrieve messages without entering an ID; Cisco Unity identifies a subscriber based on the extension from which the call originated; a password may be required.)
- Identified subscriber messaging (Cisco Unity automatically identifies a subscriber who leaves a message during a forwarded internal call, based on the extension from which the call originated.)
- Message Waiting Indicator (MWI)

Cisco Unity Outside Caller Call Flow

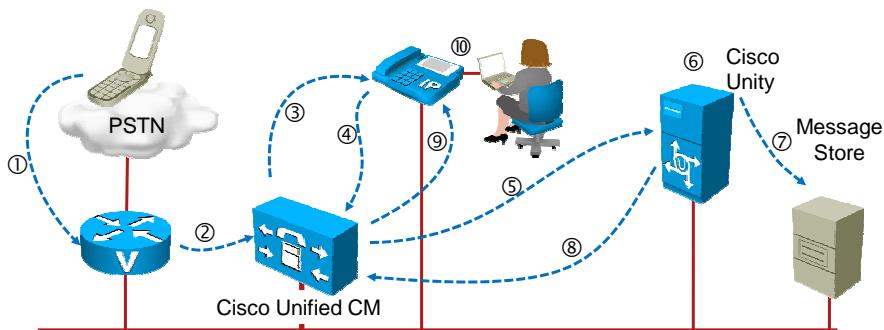
This subtopic describes how calls are routed between Cisco servers and telephone switching equipment for outside callers.



An outside caller is someone who is not identified as a Cisco Unity subscriber, generally a customer who wants to reach a person at a place of business. A Cisco Unity subscriber who calls in from a phone other than their defined office extension will also be treated as an outside caller until they sign in and identify themselves. This is an example of how a call from an outside caller might flow through the system (refer to step numbers in the figure):

- Step 1** The outside caller dials a phone number from their cell phone. The phone number dialed is a direct inward dialing (DID) number that belongs to a Cisco Unity subscriber.
- Step 2** The public switched telephone network (PSTN) routes the caller to the office communication equipment.
- Step 3** The DID number is programmed to ring a phone extension. Based on DID information provided by the PSTN, the Cisco Unified Communications Manager sends the incoming call to the telephone that it is programmed for that DID number.
- Step 4** The telephone rings four times, but the subscriber does not answer the phone because they are busy.
- Step 5** The Cisco Unified Communications Manager has been programmed to forward any unanswered calls to voice-mail after four rings. The telephone system forwards the outside caller to the voice-mail system.

Cisco Unity Outside Caller Call Flow (Cont.)



6. Cisco Unity plays a greeting message and takes the message from the outside caller.
7. Message is stored in subscriber message store.
8. Cisco Unity sends the code to turn on the MWI light on the phone.
9. Cisco Unified CM instructs the phone to turn on the MWI light.
10. On the phone, MWI light comes on.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-8

- Step 6** Cisco Unity plays a greeting message and takes the message from the outside caller.
- Step 7** Message is stored in subscriber message store.
- Step 8** Cisco Unity sends the code to turn on the MWI light on the phone to the Cisco Unified Communications Manager.
- Step 9** Cisco Unified Communications Manager instructs the phone to turn on the MWI light.
- Step 10** On the phone, the MWI light comes on.

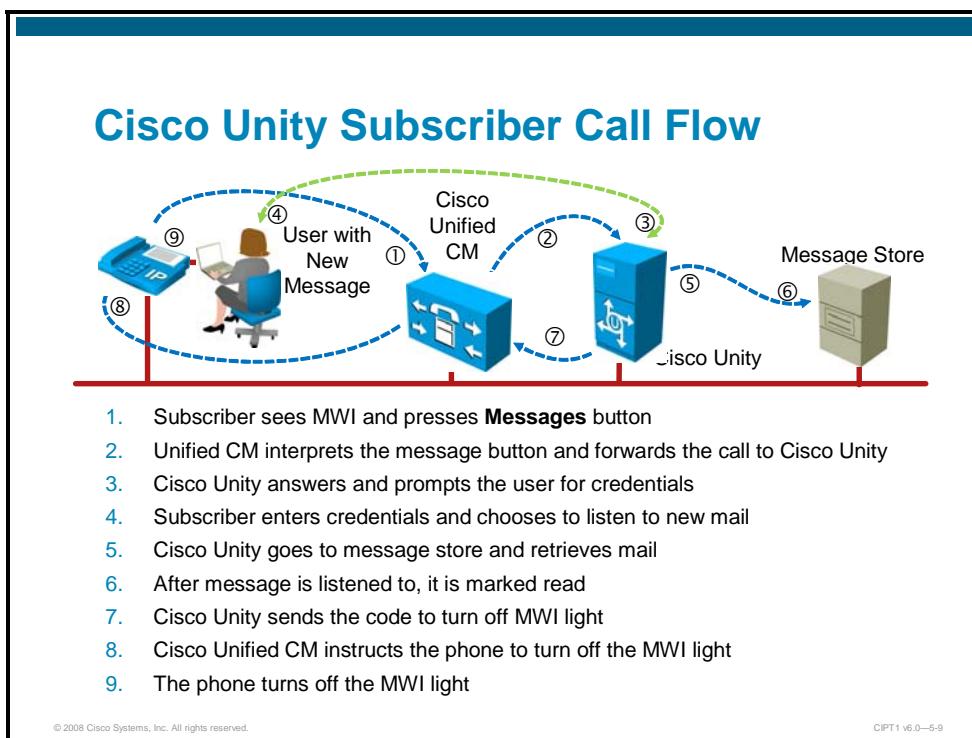
For this scenario to work, calling privileges (partitions and calling search spaces [CSSs]) must be assigned to the voice-mail ports, gateways, phones, and MWI ports.

The voice-mail ports need to reach all phones, the other voice-mail ports, the MWI ports, and the PSTN if forwarding to PSTN destinations is possible. In addition, these reaches must be made:

- The gateway must be able to reach the phones and the voice-mail ports.
- The phones have to be able to reach the voice-mail ports.
- The MWI ports have to be able to reach the phones.

Cisco Unity Subscriber Call Flow

This subtopic describes how calls are routed between Cisco servers and telephone switching equipment for subscribers.



A Cisco Unity subscriber is a person who has a user account on the Cisco Unity system. Each subscriber account has a Profile page that stores specific information about that subscriber, such as the extension, security code, recorded name, and the e-mail alias to send messages to. In this example (refer to step numbers in the figure):

- The subscriber notices the MWI on their telephone and calls the voice-mail system to retrieve messages.
- The telephone system directs the call and the caller information (the telephone extension) to the Cisco Unity system.
- Cisco Unity receives the call and the extension of the telephone from the telephone system. Cisco Unity recognizes the extension from its list of subscribers and accesses the subscriber e-mail message store to retrieve the voice message. Cisco Unity asks the subscriber to enter their password. After the password is entered, Cisco Unity will offer to play the message for the subscriber.
- The subscriber chooses to listen to the message. Cisco Unity plays it and then offers a menu of actions to take with the message, such as “save as new,” “delete,” or “forward.” The subscriber presses “3” to delete the message and Cisco Unity verbally confirms that the message is deleted. The subscriber then hangs up the phone.
- Cisco Unity sends the subscriber delete message command to the message store server. The message will be deleted or moved to the Deleted Items folder based on settings in the subscriber account.

Voice-Mail Integration Parameters

This subtopic discusses the configuration parameters for SCCP integration, for both the Cisco Unified Communications Manager side and the corresponding setting on the Cisco Unity side of the integration.

Voice-Mail Integration Parameters

Cisco Unified CM parameter	Cisco Unity parameter
Number of Voice-Mail Ports	Number of Voice-Mail Ports
Message Waiting Information	MWI on/off Extension
Voice-Mail Port Name	CallManager Device Name Prefix
Line Directory Number	Subscriber Extension
Hunt List, Hunt Pilot, Voice-Mail Pilot, Voicemail Profile	-

© 2008 Cisco Systems, Inc. All rights reserved.
CIPT1 v6.0—5-10

Configuration starts on both systems with the creation of voice-mail ports. The number of ports depends on system load and on the number of subscribers. The name of the Voice-Mail Ports configured in Cisco Unified Communications Manager must match the CallManager Device Name Prefix Parameter on the Cisco Unity side.

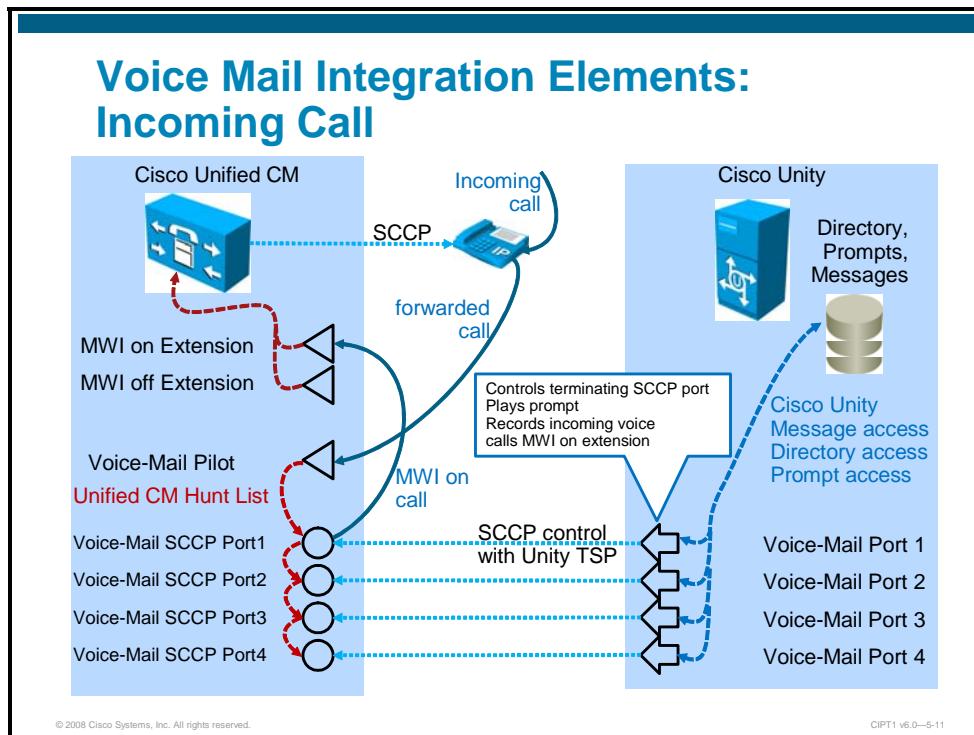
Next, in Cisco Unified Communications Manager, you must define the information about Message Waiting extensions. These extensions must match the configuration on the Cisco Unity side.

The extension of a subscriber on the Cisco Unity side equals the directory number on the line of the phone in Cisco Unified Communications Manager.

In Cisco Unified Communications Manager, each phone line is assigned to a voice-mail profile. The voice-mail profile refers to a voice-mail pilot, which is configured with the number of a hunt pilot (that is, the number that is used to access the voice-mail system). The hunt pilot refers to a hunt list, which includes a line group that consists of the directory numbers of the individual voice-mail ports.

Voice Mail Integration Elements: Incoming Call

The figure shows the interaction of Cisco Unity and Cisco Unified Communications Manager elements on a forwarded call to a voice-mail subscriber.



Any incoming call which is forwarded to voice mail will reach the voice-mail pilot number assigned to the hunt pilot of the voice-mail hunt list.

The voice-mail hunt list will select the voice-mail port that is terminating the incoming call.

The voice-mail ports in the Cisco Unified Communications Manager are specialized SCCP-controlled computer telephony integration (CTI) ports. These ports are in control of the related Cisco Unity voice-mail ports via the Cisco Unity-Cisco Unified Communications Manager Telephony Application Programming Interface (TAPI) Service Provider (TSP).

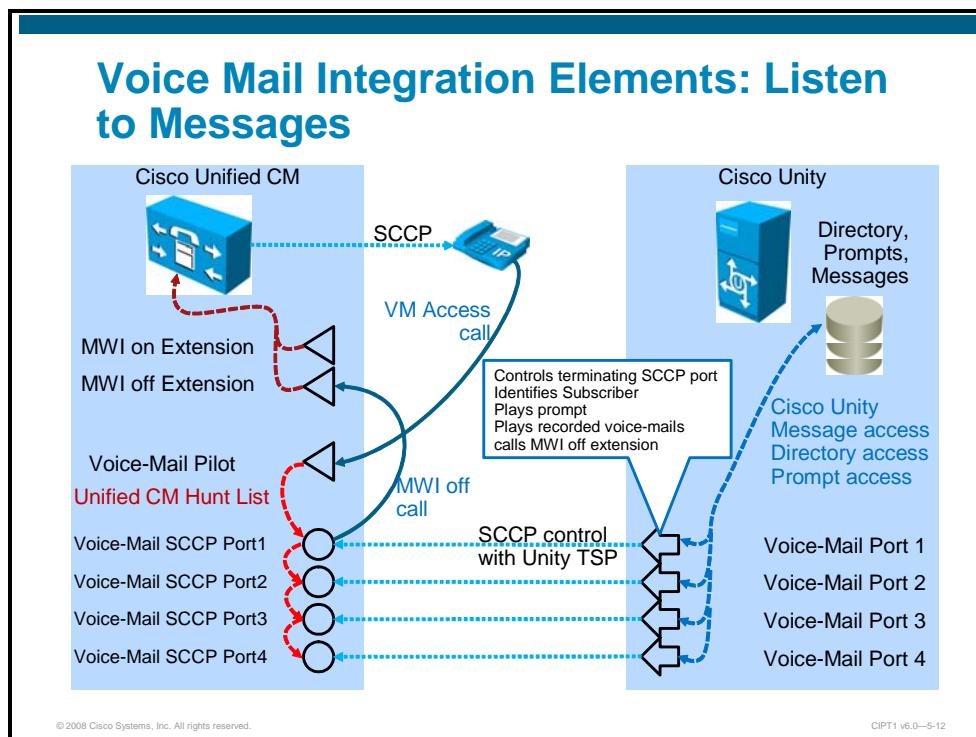
Using the voice-mail ports, Cisco Unity connects the call, playing prompts and recording messages.

After finishing the recording of messages, Cisco Unity initiates a call to the MWI on extension. The signaling of the call contains the number of the extension, which must switch on the message waiting lamp.

Cisco Unified Communications Manager then instructs the indicated phone to activate MWI.

Voice Mail Integration Elements: Listen to Messages

The figure shows the interaction of Cisco Unity and Cisco Unified Communications Manager elements on a call for voice-mail access.



An internal call to the voice-mail reaches the voice-mail pilot number assigned to the hunt pilot of the voice-mail hunt list.

The voice-mail hunt list selects the voice-mail port that is terminating the incoming call.

The voice-mail ports in the Cisco Unified Communications Manager are specialized SCCP-controlled CTI ports. These ports are in control of the related Cisco Unity voice-mail ports via the Cisco Unity-CM TSP.

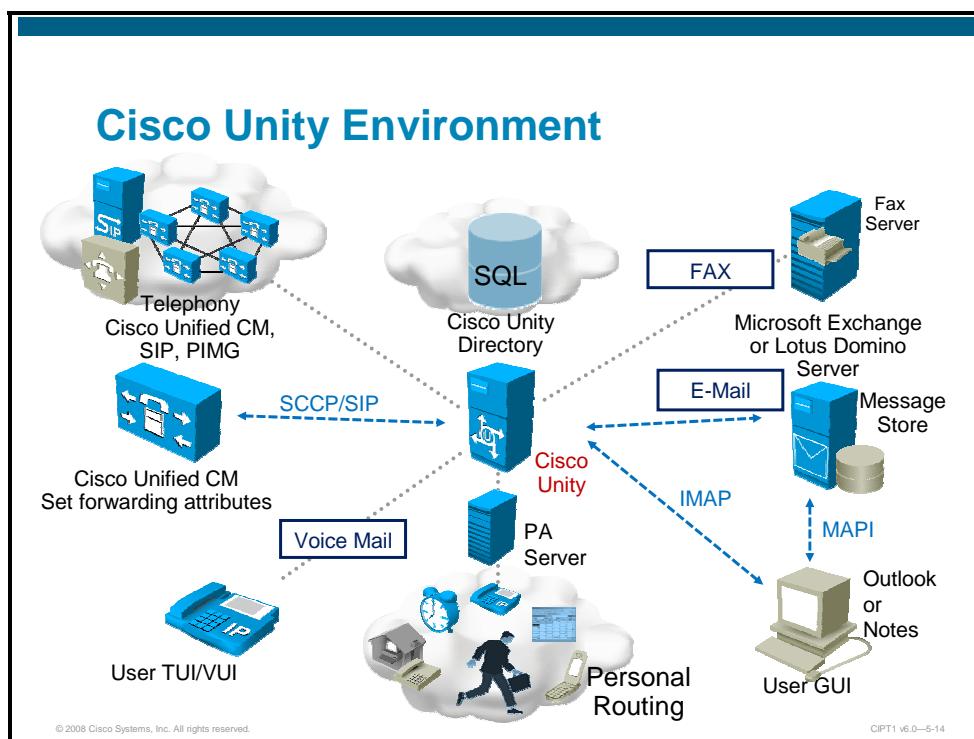
Using the voice-mail ports, Cisco Unity connects the call, identifying the user, playing prompts, and playing back the messages.

When messages are deleted, Cisco Unity initiates a call to the MWI off-extension. The signaling of the call contains the number of the extension which has to switch the message waiting lamp off.

Cisco Unified Communications Manager then instructs the indicated phone to deactivate MWI.

Cisco Unity Components

This topic describes the components of Cisco Unity and their functions.



Cisco Unity is a powerful and intelligent voice messaging system. With Cisco Unity Unified Messaging, e-mails can be listened to over the telephone, voice messages can be checked from the Internet, and, when integrated with a supported third-party fax server, faxes can be forwarded to any location.

Cisco Unity integrates seamlessly with a Microsoft Outlook e-mail client to handle all messages—e-mail, voice, and fax. Cisco Unity uses Microsoft Exchange message store and directory services to unify system administration, collecting all messages in a single store and providing a single address directory service.

With Cisco Personal Assistant, users can manage how and where they want to be reached using web-based and telephone user administration interfaces. Cisco Personal Assistant offers personal call rules, speech recognition, and productivity services for IP phones. Cisco Personal Assistant interoperates with Cisco Unified Communications Manager and Cisco Unity.

Cisco Unified Communications Manager is the software-based call-processing component of the Cisco Unified Communications solution. This software extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, VoIP gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems interact with the IP telephony solution through Cisco Unified Communications Manager open telephony application programming interface (API).

Cisco Unity Standard Features

Cisco Unity is a Windows-based communications solution that brings you voice-mail and unified messaging, and integrates them with the desktop applications used every day. Cisco Unity works with Microsoft Exchange to deliver and store all messages—voice, fax, and e-mail—giving users the ability to access all of their messages by using a desktop PC, a touch-tone phone, or the Internet.

Cisco Unity Standard Features

- Intelligent voice mail
- Cisco Unity Administrator
- Cisco Personal Communications Assistant
- Cisco Unity Assistant
- ViewMail for Outlook
- Cisco Unity Inbox
- Multiple languages
- Text-to-Speech
- Third-party Fax
- Digital networking
- AMIS support
- Cisco Unity Bridge
- Enhanced failover

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-15

Cisco Unity is the unified messaging component within the Cisco family of Cisco Unified Communications system offerings, and it integrates with Cisco Unified Communications Manager, the call-processing component of Cisco Unified Communications system. Although designed for a VoIP environment, Cisco Unity also integrates with several traditional, circuit-switched phone systems. When a telephone network is ready to transition to VoIP, Cisco Unity allows migration in stages, by setting up dual phone system integration with both the circuit-switched phone system and Cisco Unified Communications Manager.

Cisco Unity includes the following features (not all of these features may be available on a particular system):

- **Intelligent voice mail:** The Cisco Unity voice messaging capabilities allow subscribers to listen to their messages, send voice messages to other subscribers, and customize settings such as personal greetings. With Cisco Unity, users can set up an automated attendant, which serves as an electronic receptionist that answers and routes incoming calls.
- **Cisco Unity Administrator:** The web administrator allows users access to the Cisco Unity server via an intranet and remotely. The Cisco Unity Administrator is used to create or modify subscriber accounts, configure messaging options, assign classes of service, record greetings, and run reports.
- **Cisco Personal Communications Assistant:** The Cisco Personal Communications Assistant (PCA) is a website that subscribers use to access the Cisco Unity Assistant and the Cisco Unity Inbox.

- **Cisco Unity Assistant:** The Cisco Unity Assistant is a website that gives subscribers the ability to customize personal settings on their computers, including recorded greetings and message delivery options. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the Active Assistant.)
- **ViewMail for Outlook:** ViewMail for Microsoft Outlook lets subscribers listen to voice messages from their Outlook Inboxes by using VCR-style controls.
- **Cisco Unity Inbox:** The Cisco Unity Inbox website lets subscribers listen to, compose, reply to, forward, and delete voice messages. (Note that in version 3.1 and earlier, the Cisco Unity Inbox was known as Cisco Unity Visual Messaging Interface).
- **Multiple languages:** With multiple languages installed, users can change the language in which Cisco Unity plays system prompts to subscribers and callers. Users can also choose one or more languages with which to display the Cisco Unity Administrator pages and the Help files.
- **Text-to-Speech:** The text-to-speech feature allows users to listen to your e-mail over the phone. Cisco Unity reads the text portion of e-mail messages and provides additional information such as the name of the sender (if the sender is a subscriber), and the time and date that the message was sent.
- **Third-party fax:** Cisco Unity supports fax servers that have dedicated fax lines set up to the fax ports on the fax server. When a third-party fax server is used with Cisco Unity, the administration of the fax server is controlled by the fax server software. You can find a list of officially supported fax servers that you can use with Cisco Unity in Supported Hardware and Software, and Support Policies for Cisco Unity Release 5.x, available on Cisco.com at
http://www.cisco.com/en/US/docs/voice_ip_comm/unity/5x/support/5xcusupp.html
- **Digital networking:** The digital networking feature enables subscribers to send and receive voice messages between Cisco Unity servers at different locations, between a Cisco Unity server and the Internet, and between a Cisco Unity server and another messaging system.
- **AMIS support:** Cisco Unity supports the Audio Messaging Interchange Specification (AMIS) protocol, which provides an analog mechanism for transferring voice messages between different voice messaging systems. A list of voice messaging systems with which Cisco Unity can exchange AMIS voice messages can be found in Cisco Unity System Requirements, and Supported Hardware and Software, available on Cisco.com at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html .
- **Cisco Unity Bridge:** The Cisco Unity Bridge acts as a networking gateway between Cisco Unity and an Octel system on an Octel analog network. With the Cisco Unity Bridge, subscribers can send messages to and receive messages from Octel users.
- **Enhanced failover:** Failover is a feature that provides a simple redundancy, allowing voice messaging functions to continue if the Cisco Unity server fails or when users need to perform maintenance. To set up failover, Cisco Unity should be installed and configured on two servers, a primary server and a secondary server. If the primary server fails or if the Cisco Unity service on the primary server stops, the secondary Cisco Unity server automatically starts performing standard Cisco Unity operations.
- **VPIM networking:** Cisco Unity supports the Voice Profile for Internet Mail (VPIM) protocol, which allows different voice messaging systems to exchange voice, fax, and text messages over the Internet or any TCP/IP network. VPIM is based on the Simple Mail Transfer Protocol (SMTP) and Multipurpose Internet Mail Extension (MIME) protocols. VPIM Networking is a licensed feature. If your organization has multiple Cisco Unity servers networked together, only one server needs to be licensed and configured for VPIM

networking. The Cisco Unity server configured for VPIM networking is referred to as the bridgehead server.

Cisco Unity Release 5.0 Additional Features

This subtopic lists the new features of Cisco Unity introduced with Release 5.0.

Cisco Unity 5.0 Release Additional Features

- Secure messaging
- Message Monitor
- Interrupt Message Recovery
- Cisco Unity Phone View
- Speech Access
- Microsoft Exchange 2007 support

© 2008 Cisco Systems, Inc. All rights reserved.

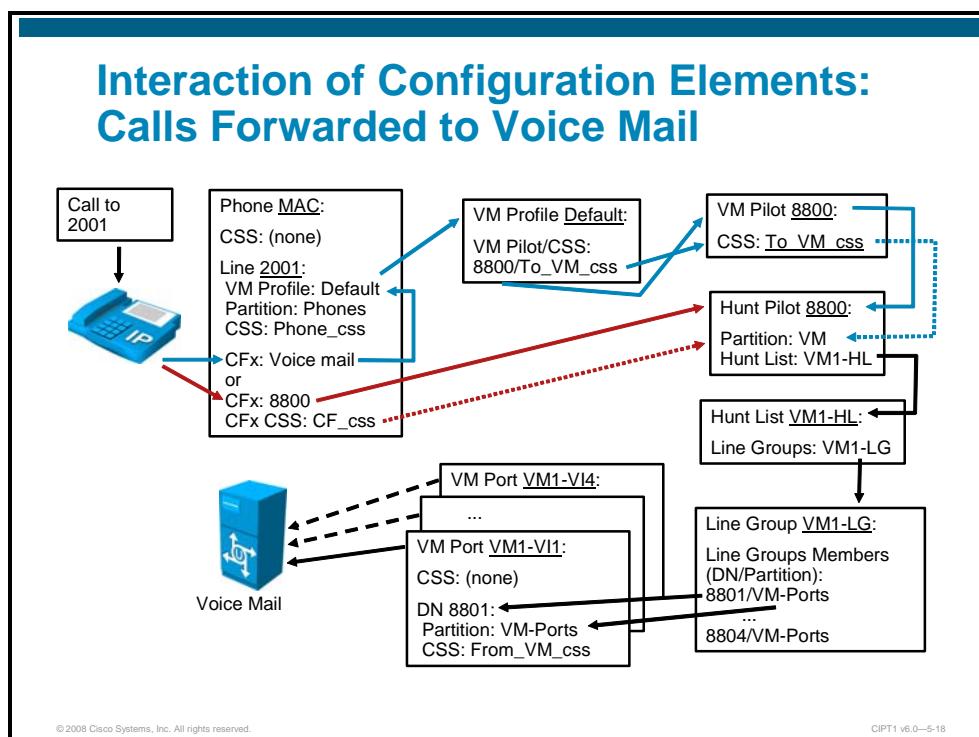
CIPT1 v6.0—5-16

These new features are available in Cisco Unity Release 5.0:

- **Secure messaging:** Encryption of voice-mail messages increases system security, allowing system administrators to enforce voice-mail retention policies and prevent the compromise of voice messages with proprietary or confidential content being forwarded to someone outside the enterprise.
- **Message Monitor:** Voice-mail messages can be screened as they are being recorded.
- **Interrupted Session Recovery:** Automatically return to in-progress message composition or playback if a session is ended prematurely, such as, for example, when someone stops by a user office with a quick question and the user hangs up the phone while in the middle of a message.
- **Cisco Unity phone view:** Users can access their voice-mail inbox through the IP phone interface. They can use the message locator to view the voice-mail message queue or jump to a particular message in their inbox, view message header details, and play selected messages.
- **Speech Access:** Press or Say capability enables the use of voice commands to navigate menus and manage voice-mail messages.
- **Microsoft Exchange 2007 support:** Microsoft Exchange 2007 can be used with Cisco Unity as a unified messaging solution (refer to *Cisco Unity System Requirements* document for more information about specific deployment models).

Cisco Unified Communications Manager Configuration for Voice-Mail Integration

This topic describes the configuration procedure for Cisco Unified Communications Manager SCCP voice-mail integration.



The figure shows the interaction of configuration elements for calls that are forwarded to voice mail.

A call is placed to directory number 2001. The corresponding phone line is forwarded to voice mail, which can be done in two different ways:

- **Forward to voice mail by activating the Forward to Voice Mail check box:** If the Forward to Voice Mail check box is activated, the voice-mail profile of the line (*Default* in this example) is used to determine where to forward the call. The voice-mail profile is configured with a voice-mail pilot number and CSS. The voice-mail pilot that matches the number and CSS specified in the voice profile (8800 and *To_VM_css* in this example) is now used to route the call. The specified voice-mail pilot number is looked up in the call routing table using the specified CSS. Therefore, the configured CSS (*To_VM_css*) must include the partition of the hunt pilot that is used to access the voice-mail system (VM in this example).
- **Forward to voice mail by specifying the hunt pilot number (8800) used for voice-mail access:** In this case, the number of the hunt pilot used for voice mail is specified at the line call forward configuration instead of activating the Forward to Voice Mail check box. When a number is entered as a call forward destination for a line, a call forward CSS can also be configured. In the example, CSS *CF_css* is configured and it must include the partition of the hunt pilot number 8800 (VM) that is specified as a call forward destination.

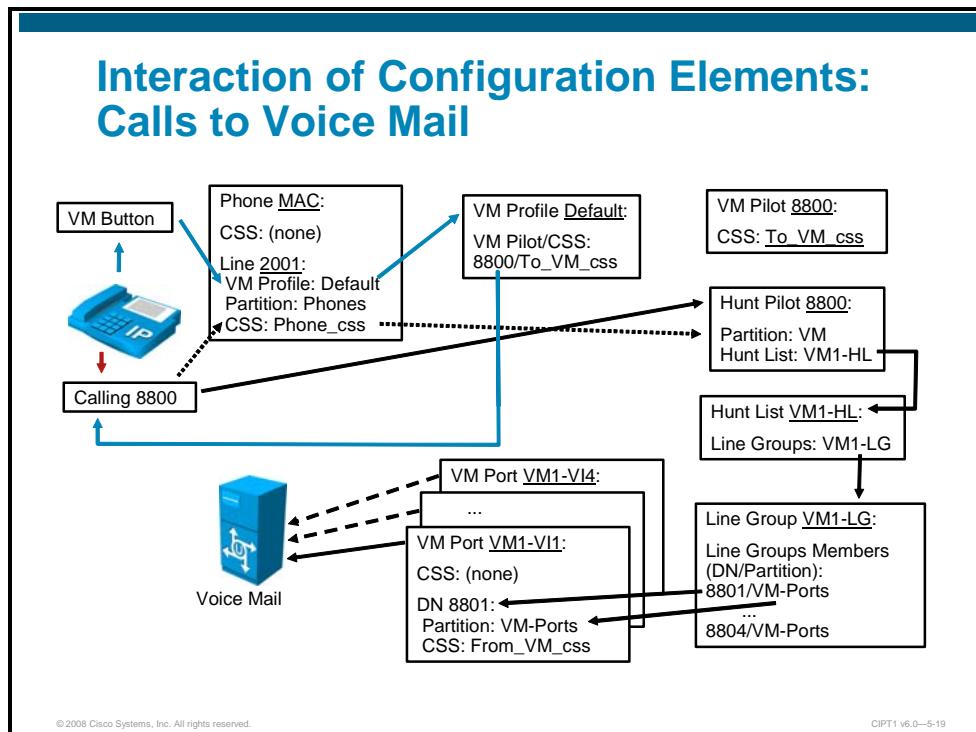
Once the call hits the hunt pilot, it is passed on to the configured hunt list (*VM1-HL* in this example). The hunt list passes the call on to the configured line group(s). In the example, only one line group is configured (*VM1-LG*), which includes four line group members: 8801 to 8804, all in partition *VM-Ports*. The line group member that is selected by the hunting algorithm (8801 in this case) is used for the communication to the voice-mail system.

Note The voice-mail pilot number and CSS in the voice-mail profile are references to identify the voice-mail pilot number to be used. They are not used to route a call; therefore there is no partition and CSS pair for this reference. The same applies to line group members that are specified by number and partition.

Note All other partitions and CSSs that are shown in the figure (such as the partition and line CSS of line 2001, the device CSS of the phone, the CSS of the voice-mail port, and the CSS of the line of the voice-mail port) are not used for calls that are forwarded to the voice-mail system. They are only shown for completeness.

Interaction of Configuration Elements: Calls To Voice Mail

This subtopic describes the interaction of configuration elements for calls to the voice-mail system.



The following elements are used to configure calls *to* the voice-mail system in the example shown in the figure:

- **IP phone:** The IP phone is configured with a line CSS *Phone_css*. The directory number of the phone is in partition *Phones*. The directory number refers to a voice-mail profile *Default*.

Note The phone can have a CSS at the device level, the line level, or both. In this example, for simplicity only one CSS (at the line) is used. The partition of the directory number of the IP phone is not relevant for calls *to* the voice-mail system. It is only considered for calls coming *from* the voice-mail system (call transfers or message notifications) to the directory number of the IP phone. The CSS of the phone (device or line CSS) is used to access the hunt pilot number (8800) and therefore needs to include the partition of the hunt pilot (VM).

- **Voice mail profile:** A voice-mail profile *Default* exists, which refers to a voice-mail pilot and CSS combination of *8800/To_VM_css*.

Note The CSS configured at the voice-mail profile is not relevant for accessing the voice-mail system from an IP phone. Only the number of the voice-mail pilot (which is also the number of the hunt mail pilot used to access the voice-mail system) is relevant.

- **Voice-mail pilot:** A voice-mail pilot that refers to a hunt pilot 8800 exists. The voice pilot is configured with a CSS *To_VM_css*.

Note	The voice-mail pilot is not used at all when accessing the voice-mail system from an IP phone. It is only used for forwarded calls when the Forward to Voice Mail checkbox is activated.
	<ul style="list-style-type: none"> ■ Hunt pilot: A hunt pilot 8800 exists in partition VM, which refers to a hunt list VM1-HL. ■ Hunt list: A hunt list VM1-HL exists. It consists of one line group: VM1-LG. ■ Line group: A line group VM1-LG exists. It includes the following directory number and partition combinations: 8001/VM-Ports, 8002/VM-Ports, 8003/VM-Ports, and 8004/VM-Ports. ■ Voice-mail port: Four voice-mail ports exist: VM1-VI1 to VM1-VI4. Each of them has a directory number (8801 to 8804) and the directory numbers of all voice-mail ports are in partition VM-Ports. The voice-mail ports have a CSS configured at their directory number: From_VM_css.

Note	The voice-mail port can have a CSS at the device (port) level or at the line (directory number) level, or both. In this example, for simplicity, only one CSS (at the directory number) is used. For calls to the voice-mail system, the CSS of the voice-mail port and its directory number are not relevant at all. They will only be considered for calls from the voice-mail system.
-------------	--

When IP phone user hits the voice-mail button of the IP phone, the following happens:

- The voice-mail profile configured for the first line is used if the voice-mail button is pressed without selecting a line before hitting the button. If a line was selected for the call first, and only then, and the voice-mail button was pressed, the voice-mail profile configured at the line that was selected for the call is used. In the example, there is only one line. After the voice-mail button is pressed, voice-mail profile *Default* is selected and the configured voice-mail pilot number (8800) is used to dial the voice-mail system.

Note	The CSS configured at the voice-mail profile is not relevant for accessing the voice-mail system from an IP phone. It is only used for forwarded calls when the Forward to Voice Mail check box is activated.
-------------	---

- A call to number 8800 is generated and the CSS used for the call routing decision is the CSS of the phone (in this case, only a line CSS is configured: *Phone_css*; if there was a device CSS, the line and device CSS would be combined with higher priority to the line CSS).

If the user dials the number of the hunt pilot that is used for voice-mail access (8800), instead of pressing the voice-mail button, the following happens:

- The dialed number 8800 is looked up in the call routing table. The CSS that is used for the call routing decision is the line or device CSS of the calling phone; in this example, it is CSS *Phone_css*.

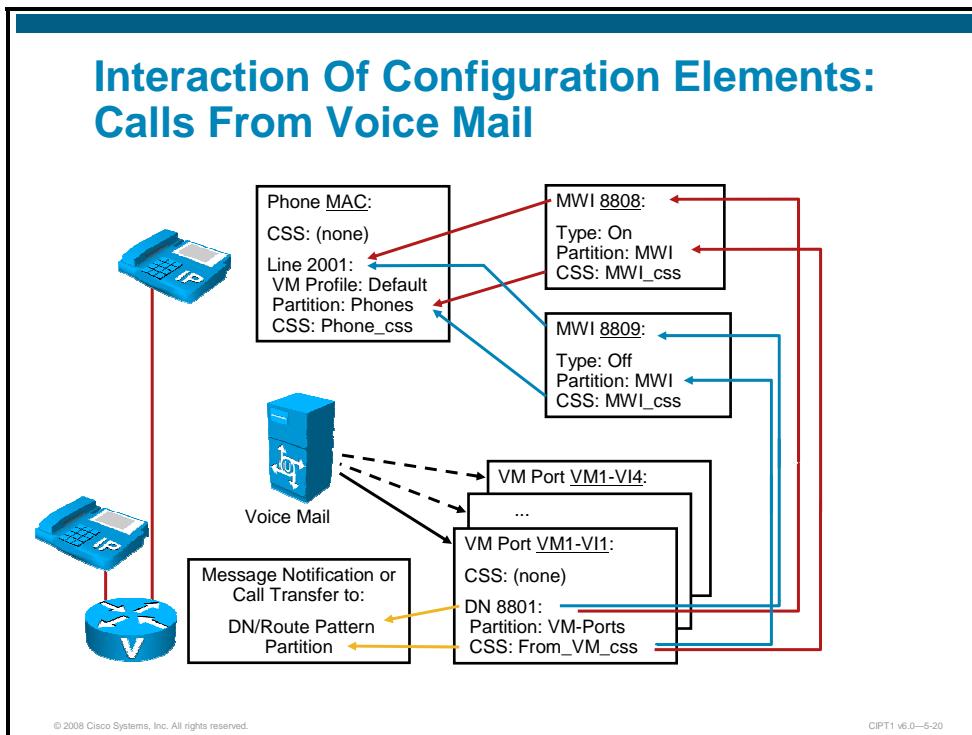
In both situations, after pressing the voice-mail button, and after directly dialing 8800, the following happens:

- Hunt pilot 8800 is found in the call routing table in partition VM (which is a partition listed in CSSs *To_VM_css* and *Phone_css*).
- The hunt pilot refers to hunt list VM1-HL. Line group VM1-LG is the only member of hunt list VM1-HL. The first available member of line group VM1-LG is 8801 in partition VM-Ports.

- The call is sent to the voice-mail system through the voice-mail port with directory number 8801 in partition *VM-Ports*.

Interaction of Configuration Elements: Calls From Voice Mail

This subtopic describes the interaction of configuration elements for calls coming from the voice-mail system.



The following elements are used to configure calls *from* the voice-mail system in the example shown in the figure:

- **Voice-mail port:** In the example, four voice-mail ports exist: VM1-VII to VM-VI4. Each of them has a directory number (8801 to 8804) and the directory numbers of all voice-mail ports are in partition VM-Ports. The voice-mail ports have a CSS configured at their directory number: *From_VM_css*.

Note For calls *from* the voice mail system, the partition of the voice-mail port directory number is not relevant.

- **MWI (on):** A message waiting number (8808) is configured for MWI on operations. The number is in partition MWI and it is configured with CSS *MWI_css*.
- **MWI (off):** A message waiting number (8809) is configured for MWI off operations. The number is in partition MWI and it is configured with CSS *MWI_css*.
- **IP phone:** The IP phone is configured with a line CSS *Phone_css*. The directory number of the phone is in partition *Phones*. The directory number refers to a voice-mail profile *Default*.

Note The device and line CSSs of the IP phone are not relevant for calls *from* the voice-mail system.

- **Other entries in the call routing table:** Several other entries in the call routing table exist, such as other phone directory numbers and route patterns. They are configured with certain partitions.

When the voice-mail system wants to turn the MWI light on or off at the IP phone, the following happens:

- The voice-mail system sends a call to the appropriate MWI number through one of the voice-mail ports (*VM1-VII* in this example).

Note This is done by calling the MWI number followed by the extension where MWI should be turned on or off (for example, to turn on the MWI light for 2001, Cisco Unity would dial 88082001).

- The device or directory number CSS, or both, of the voice-mail port is used for the call routing lookup for the dialed MWI number (8808 for MWI on).
- In the example, CSS *From_VM_css* is used and MWI on number (8808) is found in partition *MWI*, because partition *MWI* is part of the *From_VM_css* CSS.
- MWI on number 8808 now sends the on MWI to the signaled phone (2001). For this call leg, the CSS of MWI 8808, *MWI_css*, is used.
- Directory number 2001 is found in partition *Phones*, which is a partition listed in CSS *MWI_css*. The MWI light is turned on.

Note The same happens for MWI off, with the only difference being that MWI number 8809 is used.

When the voice-mail system wants to place calls to an IP phone or a route pattern in order to transfer a call or for message waiting notification, the following happens:

- The voice-mail system sends the call to the appropriate destination number through one of the voice-mail ports (*VM1-VII* in this example).
- The device or directory number CSS, or both, of the voice-mail port is used for the call routing lookup of the call.
- In the example, CSS *From_VM_css* is used, and if the dialed number is in a partition that is listed in the *From_VM_css* CSS, the call can be transferred or the message notification can be delivered.

Note The device and line CSS of voice-mail ports need access to MWI numbers and to all destinations to which calls can be transferred or to which message waiting notifications should be sent.

Note MWI numbers and voice-mail ports are put into dedicated partitions in order to be able to prevent users from dialing MWI numbers or individual voice-mail ports. Therefore, IP phones should not have access to these partitions (MWI is not required and voice-mail ports should be dialed via the appropriate hunt pilot number).

SCCP Voice-Mail Integration Configuration Procedure

This subtopic describes the configuration steps for SCCP voice-mail integration.

SCCP Voice-Mail Integration Configuration Procedure

Cisco Unified Communications Manager SCCP Integration Tasks:

1. Create MWI extensions
2. Create voice-mail ports
3. Create line group
4. Create hunt list
5. Create hunt pilot
6. Create voice-mail-pilot
7. Create voice-mail-profile

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-21

To prepare Cisco Unified Communications Manager to integrate with a Cisco Unity voice-mail system using SCCP, follow these steps:

- Step 1** Create MWI extensions
Step 2 Create voice-mail ports
Step 3 Create a line group
Step 4 Create a hunt list
Step 5 Create a hunt pilot
Step 6 Create a voice-mail pilot
Step 7 Create a voice-mail profile

Note	Steps 2 and 3 can be performed by using the Cisco Voice Mail Port Wizard. The Cisco Voice Mail Port Wizard allows quick configuration of a large number of voice-mail ports by simply specifying the number of voice-mail ports to be created. These voice-mail ports are added and assigned to a line group. All other steps still have to be performed manually. The Cisco Voice Mail Port Wizard can be accessed from Voice Mail > Cisco Voice Mail Port Wizard .
-------------	--

Step 1: Create MWI Extensions

This subtopic describes how to add message waiting numbers.

The screenshot shows the 'Voice Mail > Message Waiting' configuration screen. It displays two separate configuration forms for 'Message Waiting Information'.
Form 1 (Top):
- Message Waiting Number*: 8808
- Partition: MWI
- Description: MWI on
- Message Waiting Indicator*: On Off
- Calling Search Space: MWI_css
A callout box points to the 'Message Waiting Number' field with the text: 'Configure Message Waiting Number for MWI on and apply Partition and Calling Search Space'.
Form 2 (Bottom):
- Message Waiting Number*: 8809
- Partition: MWI
- Description: MWI off
- Message Waiting Indicator*: On Off
- Calling Search Space: MWI_css
A callout box points to the 'Message Waiting Number' field with the text: 'Configure Message Waiting Number for MWI off and apply Partition and Calling Search Space'.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-22

To add message waiting numbers, follow these steps:

- Step 1** In Cisco Unified Communications Manager Administration, go to **Voice Mail > Message Waiting** and click **Add New**.
- Step 2** Configure a message waiting number for MWI On by configuring a Message Waiting Number and description and setting the Message Waiting Indicator to On.
- Step 3** Repeat the previous step to create a Message Waiting Number for MWI Off.

The partition and CSSs are used in the following way: A partition at a message waiting number specifies which devices are allowed to dial the MWI number. These are voice-mail ports when trying to inform Cisco Unified Communications Manager about an MWI state change sourced by the voice-mail system. Therefore, the CSS at the voice-mail ports must include the partition of the MWI numbers.

The CSS at the MWI numbers must include the partitions of all phones whose MWI lamps should be turned on or off. Only then, MWI can set or unset the MWI light for a directory number.

Step 2: Create Voice-Mail Ports

This subtopic describes how to add voice-mail ports to Cisco Unified Communications Manager.

Step 2: Create Voice-Mail Ports

Voice Mail > Cisco Voice Mail Port

Enter Port Name, Description, and select Device Pool for the voice mail pilot

Set the Device Security Mode

Enter the directory number, Partition, and Calling Search Space of the voice-mail pilot

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-23

To add voice-mail ports, follow these steps:

- Step 1** In Cisco Unified Communications Manager Administration, go to **Voice Mail > Cisco Voice Mail Port**, and click **Add New**.
- Step 2** Configure the voice-mail port with a Port Name, Description, and select a Device Pool.

Note The Port Name has to end with “–Vlx” where x is a number starting with 1 for the first voice-mail port, 2 for the next voice-mail port, and so on.

- Step 3** Set the Device Security Mode.

Note The device security mode is a mandatory parameter and does not have a default value. Therefore it must be selected. If the Cisco Unified Communications Manager cluster has not been enabled for security, the device security mode must be set to Non Secure Voice Mail Port in order for the voice-mail port to function correctly. To enable security in the Cisco Unified Communications Manager cluster, additional hardware products (security tokens) must be purchased and the cluster has to be configured for secure operation. More information about how to enable security in a Cisco Unified Communications Manager cluster is provided in the CIPT2 course.

- Step 4** Enter a Directory Number for the voice-mail port.

Note The directory number must be a unique number within the system and is used to identify the individual voice-mail port. It will be assigned into a line group later on.

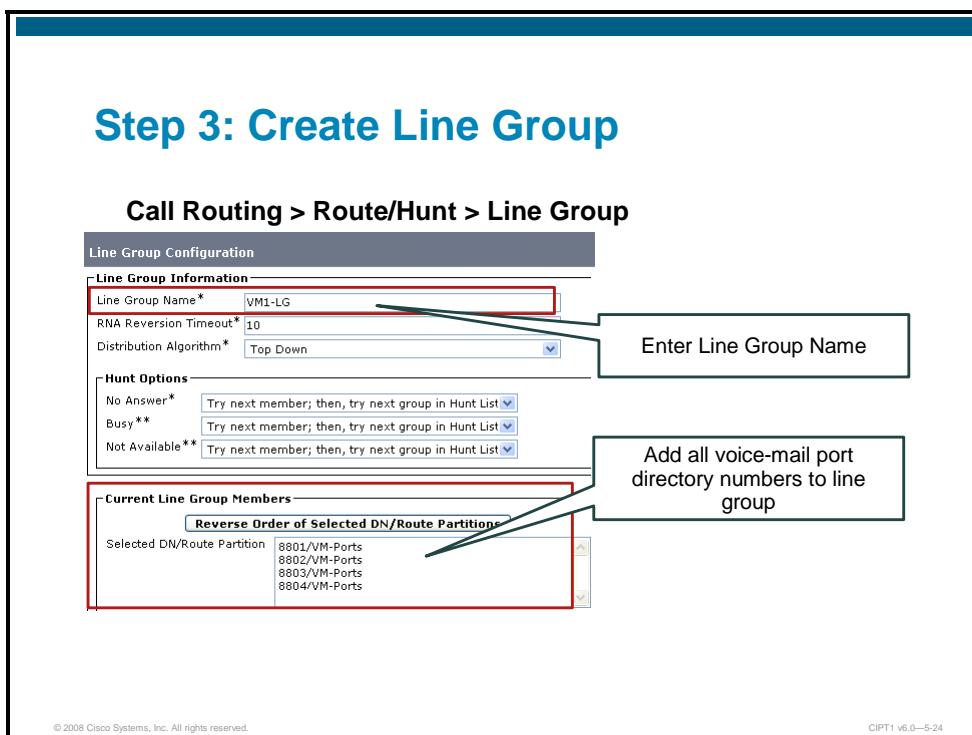
Step 5 Repeat the previous step to configure as many voice ports as desired.

Similar to an IP phone, the CSS of a voice port is composed of a device CSS (that is, the voice-port CSS) and a line CSS (that is, the directory number CSS). The partitions of the voice-port CSS have higher priority than the partitions of the voice-port directory number CSS. The combined CSS must allow calls to subscriber phones and any other number to which the voice-mail system should be able to send calls (for example, during call transfers, message notifications, and message waiting indications). These can be internal phone directory numbers, route patterns, MWI numbers, or other dialable patterns such as translation patterns.

The partition of the voice-mail port is referenced from the line group (along with the voice-mail port directory number). Line groups do not have a CSS that specifies which directory numbers can be accessed, but the combination of directory number and partition is configured at the line group.

Step 3: Create Line Group

This subtopic describes how to add a line group containing the directory numbers of the previously configured voice-mail ports.



To add a line group with voice-mail ports, follow these steps:

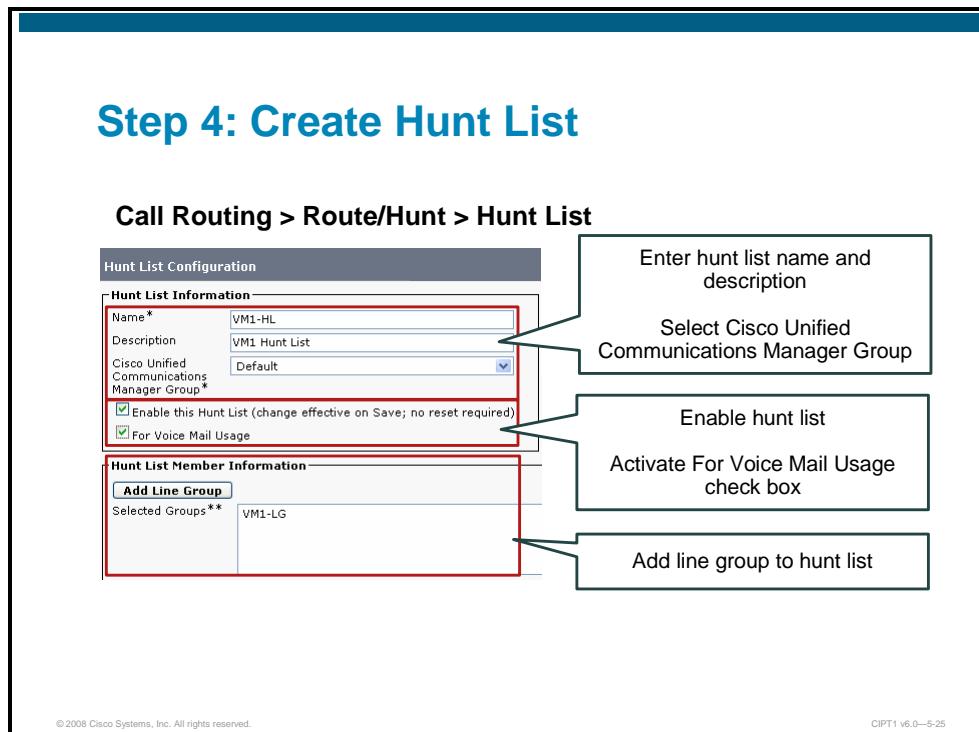
- Step 1** In Cisco Unified Communications Manager Administration, go to **Call Routing > Route/Hunt > Line Group** and click **Add New**.
- Step 2** Enter a name for the line group, select **Distribution Algorithm Top Down**, and add the directory numbers of all previously configured voice-mail ports to the line group.

The line group does not use a CSS to select line group members, but if the line-group member directory number has a partition assigned, the combination of directory number and partition is specified.

-
- Note** If some voice-mail ports should be used for dialout only (calls being transferred *from* the voice-mail system or calls used for message notifications, or message waiting indication) they must not be included in the line group. The line group should only contain the voice-mail ports that are used for calls *to* the voice-mail system.
-

Step 4: Create Hunt List

This subtopic describes how to add a hunt list that contains the previously configured line group.



To add a hunt list using the previously configured line group, follow these steps:

- Step 1** In Cisco Unified Communications Manager Administration, go to **Call Routing > Route/Hunt > Hunt List** and click **Add New**.
- Step 2** Enter a Name and Description for the hunt list and select a Cisco Unified Communications Manager Group.
- Step 3** Click the **Enable this Hunt List** check box and the **For Voice Mail Usage** check box.

Note The For Voice Mail Usage parameter addresses the problem of voice-mail calls that are rejected when a hunt list use reaches a maximum, because all voice-mail ports are in use.

On a hunt list that is used for voice messaging, activate the **For Voice Mail Usage** check box and make sure that all members of line groups that have been assigned to the hunt list are voice-mail ports.

- Step 4** Add the line group that was configured in the previous step to the hunt list.

A hunt list is neither configured with a partition nor with a CSS. The reason is that the hunt list is neither called by a number (the hunt pilot that refers to the hunt list is called by a number) nor does it place a call to a phone or voice-mail port directory number, but refers to a named line group instead (which then accesses the line group members).

Step 5: Create Hunt Pilot

This subtopic describes how to add a hunt pilot that refers to the previously configured hunt list.

The screenshot shows the 'Call Routing > Route/Hunt > Hunt Pilot' configuration page. A callout box highlights the 'Hunt Pilot number' field, which is set to '8800'. Another callout box highlights the 'Description' field, which contains 'VM1 Hunt Pilot'. A third callout box highlights the 'Select Hunt List' field, which is set to 'VM1-HL'. The interface includes various dropdown menus and checkboxes for route options like 'Route this pattern' and 'Block this pattern'.

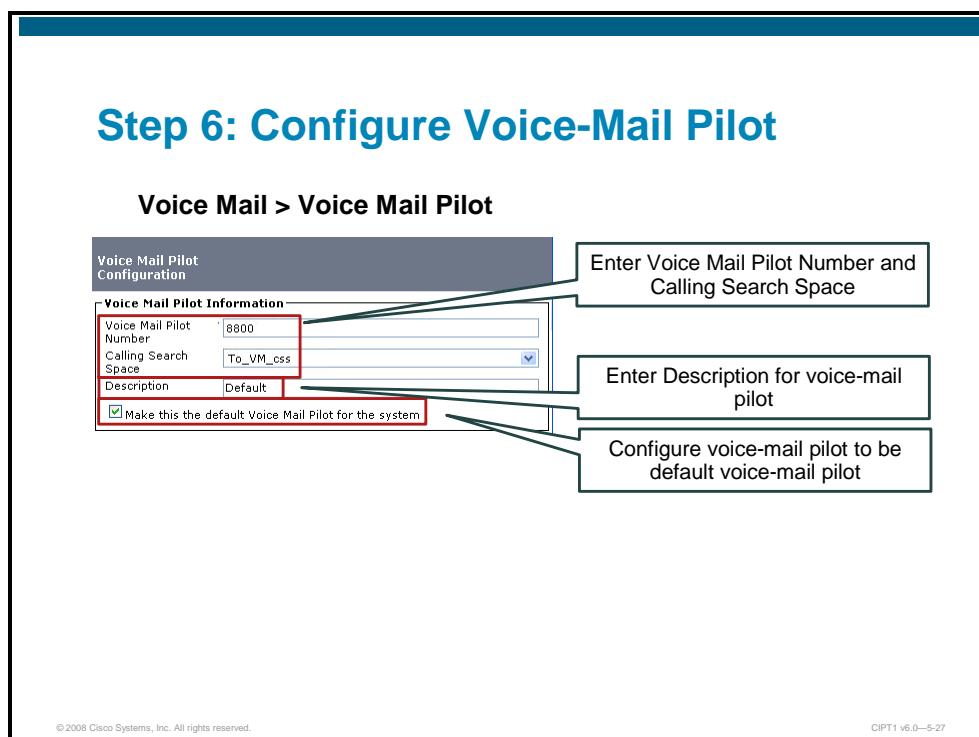
To add a hunt pilot that refers to the previously configured hunt list, follow these steps:

- Step 1** In Cisco Unified Communications Manager Administration, go to **Call Routing > Route/Hunt > Hunt Pilot** and click **Add New**.
- Step 2** Enter the Hunt Pilot number. This is the number where the voice-mail system will be reached for forwarding calls and message retrieval.
- Step 3** Enter a Description for the hunt pilot.
- Step 4** Select the Hunt List that was configured earlier.

The partition in the hunt pilot determines which devices are allowed to call the hunt pilot number. Because the hunt pilot is the number used to access the voice-mail system for forwarding calls and retrieving messages, all devices that should be able to call the voice-mail system must have this partition in their CSS. If the Forward to Voice Mail check box is activated on a phone line, the voice-mail pilot that is referenced from the voice-mail profile configured at the corresponding phone line also must have access to the hunt pilot partition. This is required because the CSS of the voice mail pilot is used to forward such calls to the voice-mail system.

Step 6: Configure Voice-Mail Pilot

This subtopic describes how to configure a voice-mail pilot that refers to the previously configured hunt pilot.



To configure a voice-mail pilot to refer to the previously configured hunt pilot, follow these steps:

- Step 1** In Cisco Unified Communications Manager Administration, go to **Voice Mail > Voice Mail Pilot** and choose to configure the Default voice-mail pilot.

Note	Two voice-mail pilots exist by default: the Default voice-mail pilot and the No Voice Mail voice-mail pilot. If only one voice-mail system is used, it is recommended to configure the Default voice-mail pilot. If multiple voice-mail systems are used, additional voice-mail pilots must be added. The No Voice Mail voice-mail pilot does not refer to any hunt pilot because it is only referenced from voice-mail pilots that do not allow voice-mail integration.
-------------	--

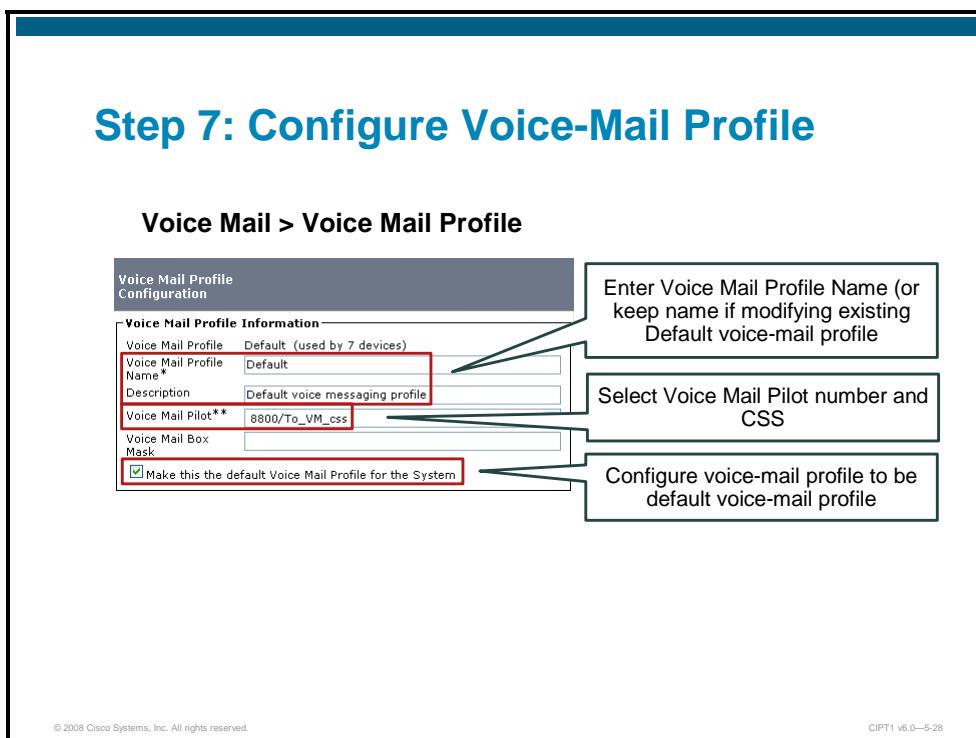
- Step 2** Enter the Voice Mail Pilot Number. This is the number of the previously configured hunt pilot.
- Step 3** Enter a Description for the voice-mail pilot.
- Step 4** Activate the **Make This the Default Voice Mail Pilot for the System** check box if desired.

Note	If multiple voice-mail pilots are used, one of them is configured to be the default voice-mail pilot. By default, the Default voice-mail pilot is configured to be the default voice-mail pilot.
-------------	--

The CSS of the voice-mail pilot is used for the voice-mail pilot to access the configured pilot number (which is the number of the hunt pilot). Therefore, the CSS must include the partition that is assigned to the hunt pilot. It is used for forwarded calls when the Forward to Voice Mail check box is activated at the phone line.

Step 7: Configure Voice-Mail Profile

This subtopic describes how to configure a voice-mail profile that refers to the previously configured voice-mail pilot.



To configure a voice-mail profile to refer to the previously configured voice-mail pilot, follow these steps:

- Step 1** In Cisco Unified Communications Manager Administration, go to **Voice Mail > Voice Mail Profile** and choose to configure the Default voice-mail pilot.

Note Two voice-mail profiles exist by default: the Default voice-mail profile and the NoVoiceMail voice-mail profile. If only one voice-mail system is used, it is recommended to configure the Default voice-mail profile. If multiple voice-mail systems are used, additional voice-mail profiles must be added. The NoVoiceMail voice-mail profile refers to the No Voice Mail voice-mail pilot, which has no reference to any hunt pilot because it does not allow voice-mail integration.

- Step 2** Enter the Voice Mail Profile Name and a Description, or keep the configured name and description if you are modifying an existing voice-mail profile, such as the Default voice-mail profile.

- Step 3** Select the previously configured voice-mail pilot.

- Step 4** Activate the **Make This the default Voice Mail Profile for the System** check box, if desired.

Note If multiple voice-mail profiles are used, one of them is configured to be the default voice-mail profile. By default, the Default voice-mail profile is configured to be the default voice-mail profile.

A voice-mail profile refers to a voice-mail pilot by the voice-mail pilot number and the CSS configured at the voice-mail pilot.

Note	Voice-mail profiles are used for forwarded calls (when the Forward to Voice Mail check box is activated at a line) or when the voice-mail button is pressed on a Cisco IP phone. They are ignored when a user directly dials the hunt pilot number that is configured to access the voice-mail system.
-------------	--

Cisco Unified Communications Manager Phone Configuration for Voice-Mail Usage

This topic describes how to configure IP phones for voice-mail usage.

Configuring Phone Lines for Voice-Mail Usage

Device > Phone > Line

Directory Number Configuration

Save Reset

Status
Status: Ready

Directory Number Information

Directory Number*: 2001
Route Partition: Phones

Directory Number Settings

Voice Mail Profile	Default
Calling Search Space	Phones_css
Presence Group*	Standard Presence group
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Auto Answer*	Auto Answer Off

Select the Voice Mail Profile at each phone line

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-30

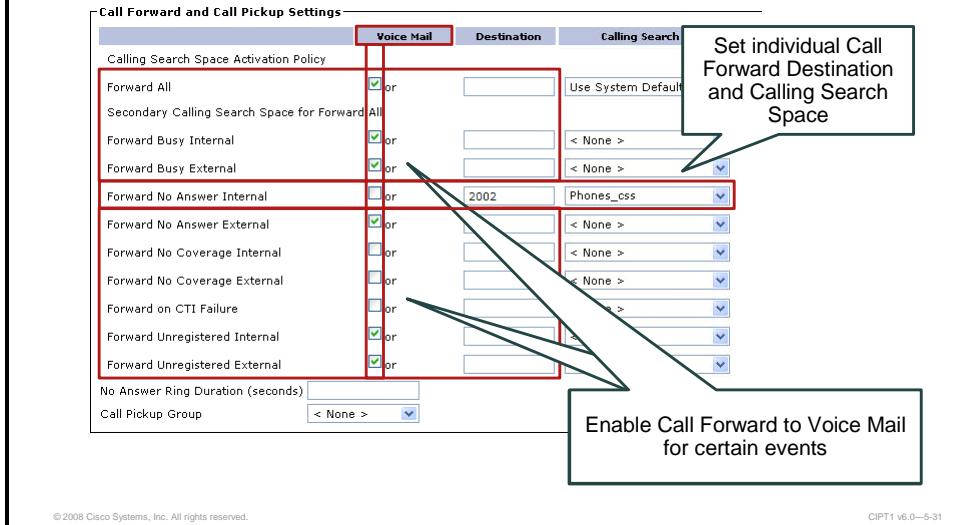
To configure phone lines to use a voice-mail system, the phone line must be configured with a voice-mail profile as described in the following steps:

- Step 1** In Cisco Unified Communications Manager Administration, go to **Device > Phone** and select the IP phone that should be configured for voice-mail usage.
- Step 2** At each phone line, select the Voice Mail Profile that should be used by the phone.

Note By default, all phone lines have the Voice Mail Profile set to Default. If only one voice-mail system is used, and the Default voice-mail profile and the Default voice-mail pilot have been configured as described in the previous topic, effectively this means that the changes performed at the Default voice-mail pilot (changing the voice-mail pilot number from blank to the number configured for the hunt pilot) immediately applies to all phones. The voice-mail profile and the phone lines do not have to be configured in this case because their default values are chosen to allow such a simple integration. This approach is recommended when integrating with a single voice-mail system.

Note Using voice-mail profiles is not mandatory. They allow the user to access the voice-mail system by pressing the voice-mail button on the Cisco IP phone instead of dialing the hunt pilot number that provides access to the voice-mail system. In addition, the use of voice-mail profiles allows call forward to voice-mail to be configured by a check box instead of specifying the hunt pilot number that refers to the voice-mail system as the call forward destination.

Configuring Phone Lines for Voice-Mail Usage (Cont.)



Finally, the phone lines have to be configured to forward calls to the voice-mail system. This can be configured at the phone (for Call Forward All), from user web pages, or by the administrator as shown in the figure.

If Call Forward All is selected, all other call forward settings are ignored. If Call Forward All is not enabled, the other call forward settings are used based on the event (busy, no answer, unregistered, and so on). Call forward no coverage only applies to lines which forwarded calls to a hunt list where hunting exhausted and the hunt pilot is configured to perform final forwarding based on the personal preference (that is, the Call Forward No Coverage parameter) configured at the phone line.

Note	If voice-mail profiles are not used, Call Forward to Voice Mail cannot be enabled by activating the check box, but must be enabled by specifying the number of the hunt pilot which provides access to the voice-mail system. When configuring a call forward destination number, a call forward CSS has to be configured when the forward destination is in a partition.
-------------	---

Cisco Unity Configuration for Cisco Unified Communications Manager Integration

This topic describes the configuration tasks for the Cisco Unified Communications Manager-Cisco Unity integration on Cisco Unity.

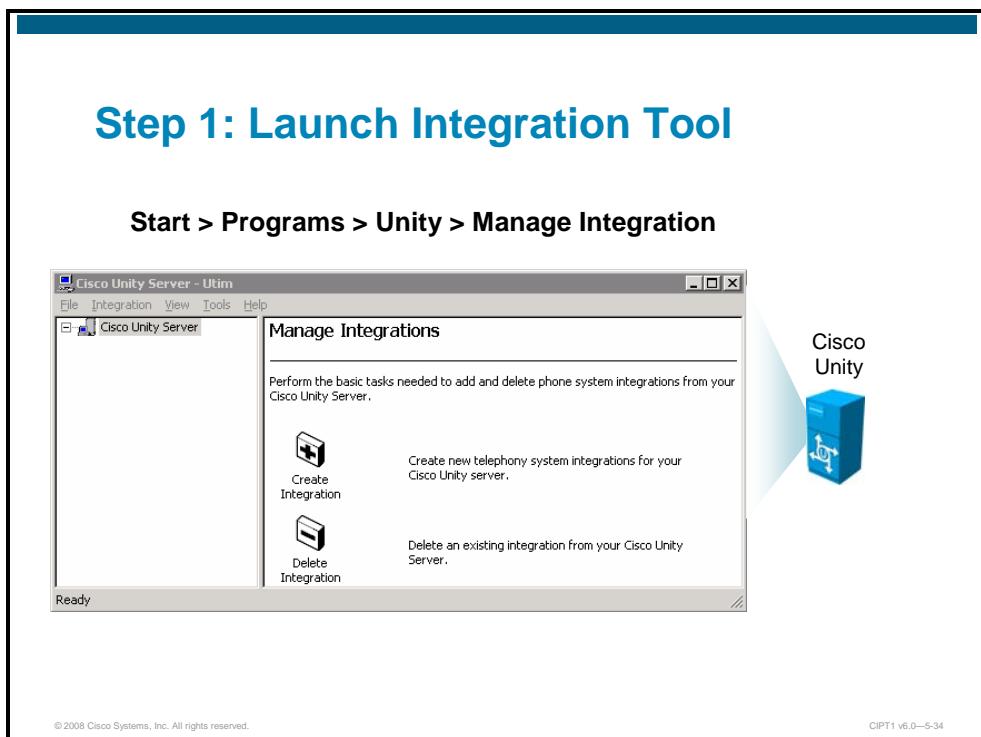
Cisco Unity SCCP Integration Configuration Tasks

1. Launch Integration tool
2. Start Integration wizard
3. Create a new SCCP Cisco Unified Communications Manager integration
4. Update Unity-CM TSP

The integration of Cisco Unity is wizard-driven.

Step 1: Launch Integration Tool

The first step to start the integration is to locate and start the Cisco Unity Telephony Integration Manager on the Cisco Unity server.



Choose the **Create Integration** option.

Step 2: SCCP Cisco Unified Communications Manager Integration

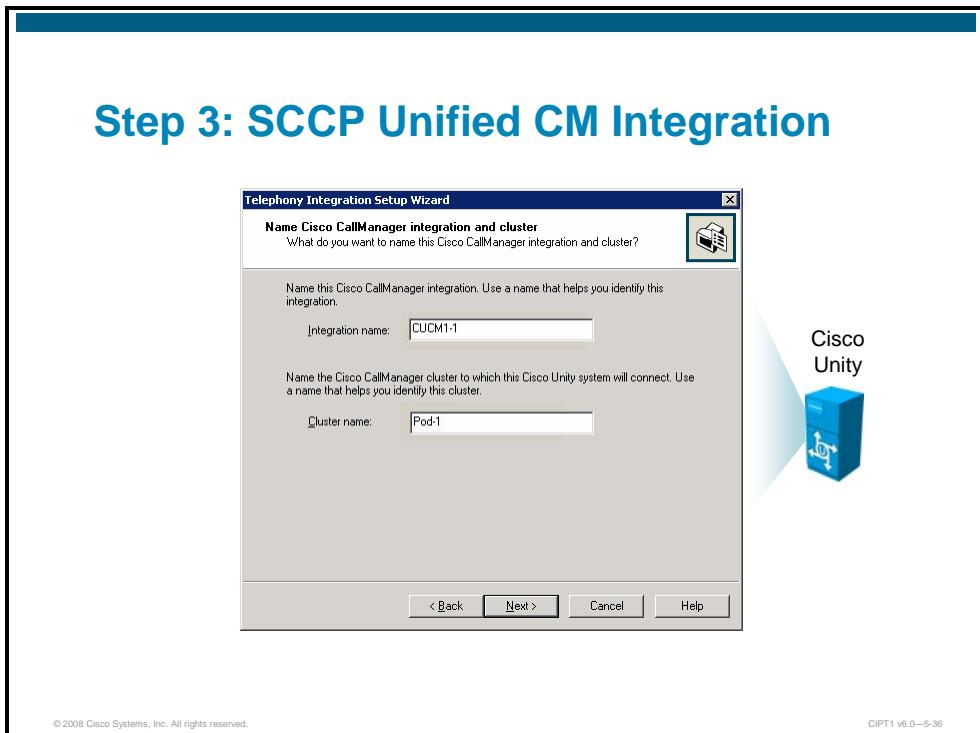
After you choose the Create Integration option in the Cisco UTIM, the Telephony Integration Setup Wizard window appears.



Click the **SCCP** radio button.

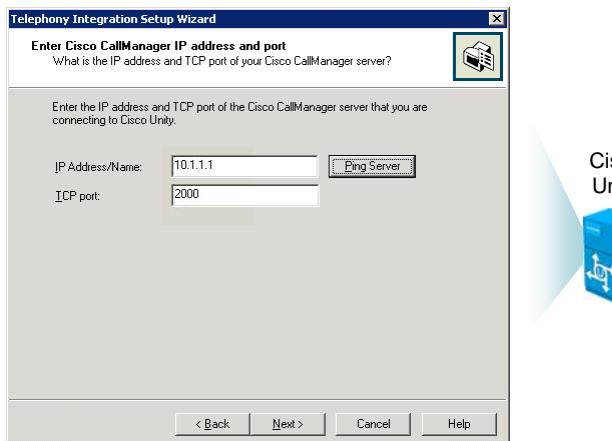
Step 3: SCCP Cisco Unified Communications Manager Integration

The final step is a restart of the Cisco Unity server.



The integration name is called Cisco CallManager; the cluster name must be entered, in addition. These settings have only local relevance on the Cisco Unity server.

Step 3: SCCP Unified CM Integration (Cont.)

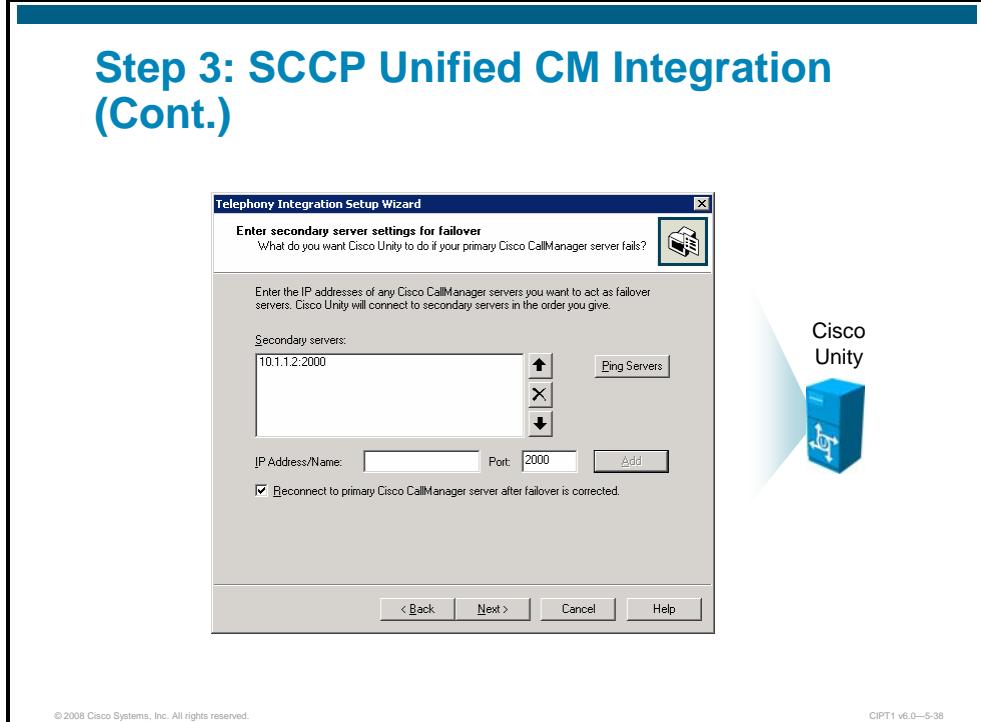


© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-37

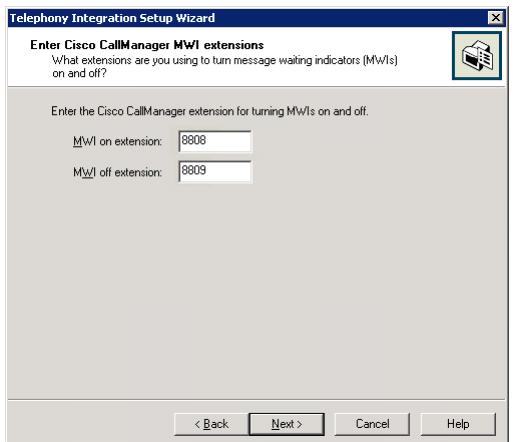
Define the IP address and the SCCP port of the Cisco Unified Communications Manager. This setting has to be completely identical with the settings in Cisco Unified Communications Manager system menu.

Step 3: SCCP Unified CM Integration (Cont.)



Define the IP address and the port number of a secondary Cisco Unified Communications Manager for redundancy, if multiple Cisco Unified Communications Manager servers exist in the cluster.

Step 3: SCCP Unified CM Integration (Cont.)

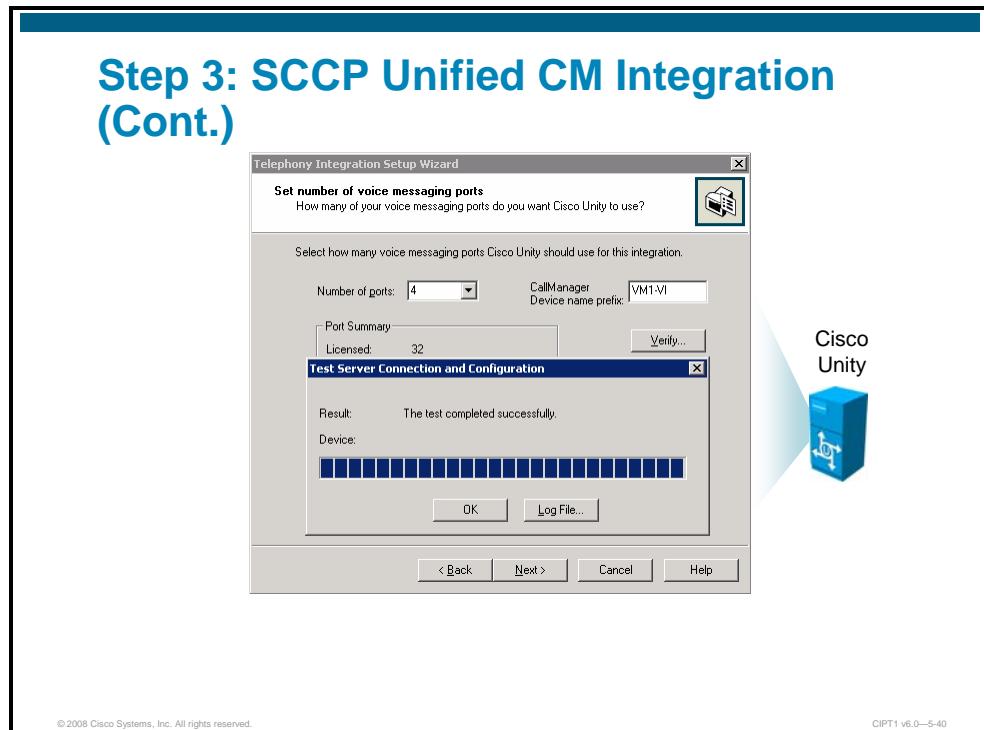


© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-39

Define which directory numbers you have defined on the Cisco Unified Communications Manager for the message waiting extensions.

Step 3: SCCP Unified CM Integration (Cont.)

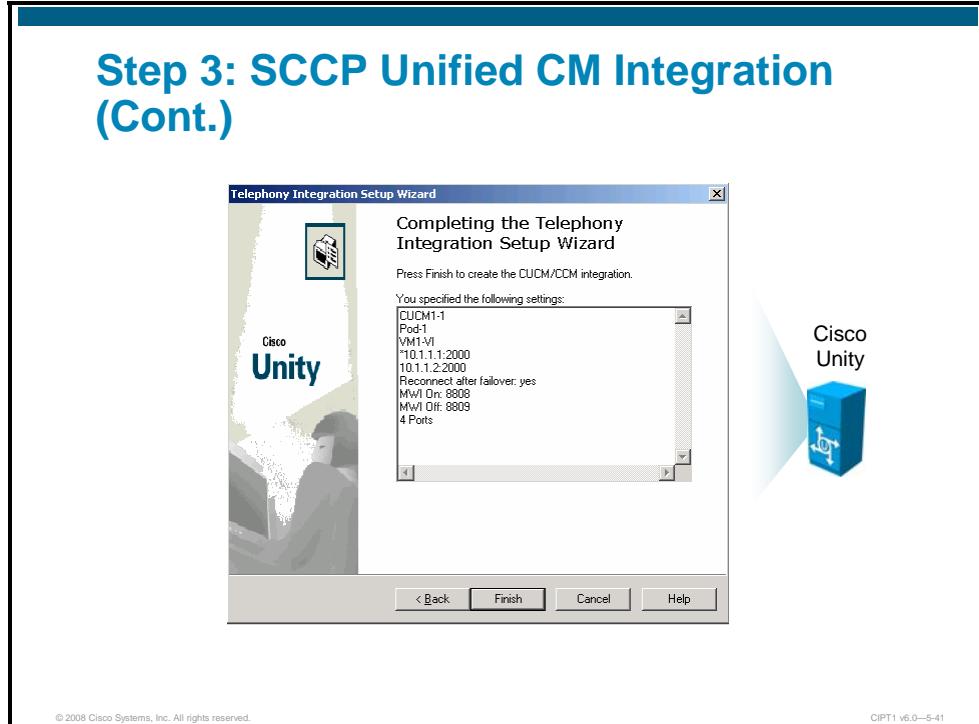


At this stage, you can perform a server connection test by clicking the **Verify** button.

Tip

Before this test, make sure that you added ports. Also ensure that the CallManager Device Name Prefix matches the setting in Cisco Unified Communications Manager.

Step 3: SCCP Unified CM Integration (Cont.)



The entered configuration settings are displayed. Verify that the information is correct. Then click **Finish** to complete the integration tasks.

Step 3: SCCP Unified CM Integration (Cont.)



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-42

The final step is the restart of Cisco Unity services.

Step 4: Update Cisco Unity-Unified Communications Manager TSP

A critical factor for a successful installation is to have a compatible version of the Cisco Unity-CM TSP installed on the Cisco Unity platform.

The screenshot shows a Windows file explorer window with the path C:\CiscoUnityCMTSP8.1.3\CiscoUnityCMTSP8.1.3. Inside this folder, there is a subfolder named "CiscoUnity-CM TSP". Within this subfolder, there is a single file named "SkinnySetup.exe". A callout bubble from the "Cisco Unity" logo points to this file. A message box is overlaid on the file list, containing the text: "To install the Cisco Unity-CM TSP, press OK. To quit, press Cancel." with "OK" and "Cancel" buttons.

- You must have a Unified CM-compatible version of the Cisco Unity-CM TSP installed on the Cisco Unity platform.
- Update the Cisco Unity-CM TSP with the Cisco Unity provided software.
- Do not use the Unified CM-provided TSP for Cisco Unity.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-43

There is a complex compatibility matrix available on <http://www.cisco.com> called “Cisco Unity SCCP Compatibility Matrix”, which helps you to determine if the Cisco Unity-CM TSP and the Cisco Unified Communications Manager are compatible. The URL to the SCCP Compatibility Matrix is as follows:

http://www.cisco.com/en/US/docs/voice_ip_comm/unity/compatibility/matrix/cutspmtx.html.

The matrix provides information about the version of the Cisco Unity-CM TSP that is required for a specific version of Cisco Unified Communications Manager. Download the appropriate version to your Cisco Unity system and then start the installation of the Cisco Unity-CM TSP.

Note Do not use the Cisco Unified Communications Manager-provided TSP for Cisco Unity.

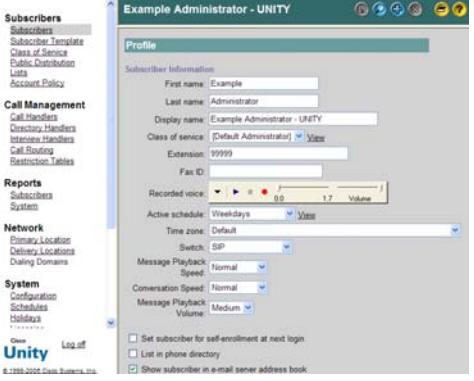
Cisco Unity Subscriber Configuration

This topic describes the creation of voice-mail boxes in Cisco Unity.

Cisco Unity User Configuration

For each phone user who needs a mailbox in Cisco Unity, a so-called subscriber needs to be created in Cisco Unity Administration. To add a subscriber, the following steps need to be performed.

1. Go to the Cisco Unity Admin web page, and log on
2. Navigate to **Subscriber** and click the + sign
3. Configure the settings: Last name, Display Name, Extension, etc.
4. Click on the floppy icon to **save**



The screenshot shows the 'Profile' configuration window in the Cisco Unity Administrator. The 'Subscriber Information' section includes fields for First name (Example), Last name (Administrator), Display name (Example Administrator - UNITY), Class of service (Default Administrator), Extension (99999), and Fax ID. The 'Network' section shows Active schedule set to Weekdays and Time zone set to Default. The 'System' section includes options for Message Playback Speed (Normal), Conversation Speed (Normal), and Message Playback Volume (Medium). At the bottom, there are three checkboxes: 'Set subscriber for self-enrollment at next login', 'List in phone directory', and 'Show subscriber in e-mail server address book'. The status bar at the bottom left says '© 2008 Cisco Systems, Inc. All rights reserved.' and the bottom right says 'CIPT1 v6.0--5-45'.

For each phone user who needs a mailbox in Cisco Unity, a so-called subscriber needs to be created in Cisco Unity Administration.

To add a subscriber, follow these steps:

- Go to the Cisco Unity Admin web page and log on.
- Navigate to **Subscribers** and click the + sign.
- Configure the settings in the Subscribers window.
- Click **Save**.

Create New User Example

This figure shows an example of a newly created user.

Create New User Example

Add Subscriber

Type of Subscriber
 New Subscriber: Exchange

Import Existing Exchange User

Note: Only Exchange subscribers have Exchange store

Subscriber Information

First name: Andreas
Last name: Szoldatics
Display name: Andreas Szoldatics
Extension: 2001
Fax ID:
Template: {Default Subscriber} Template

Exchange Information

Alias: ASzoldatics
Server: UNITY50
Mailstore: Mailbox Store (UNITY50)

Cisco Unity 

The new subscriber must be configured with an extension. The configured extension has to match the directory number that is assigned to the phone of the user in Cisco Unified Communications Manager.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco Unity is able to Integrate with multiple Cisco Unified Communications Manager clusters if they are connected via QSIG trunks.
- Cisco Unity has an Auto-Attendant function integrated.
- The voice-mail ports have to be added manually to the Hunt List.
- The voice-mail settings are assigned to the line by selecting a Voice-Mail Profile.
- The Voicemail Port Names configured in Cisco Unified Communications Manager must match the Cisco CallManager Device Name Prefix on Cisco Unity side.
- The Cisco Unity Subscriber equals a Cisco Unity user.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-47

- Cisco Unified Communications Manager can integrate with Cisco Unity, Cisco Unity Connection, Cisco Unity Express, and third-party voice mail systems.
- Cisco Unity features include Cisco Unity ViewMail for Outlook, text to speech, and secure messaging.
- Cisco Unified Communications Manager voice mail integration includes the configuration of MWI extensions, voice mail ports, line groups, hunt lists, hunt pilots, voice mail pilots, and voice mail profiles.
- Voicemail settings are assigned to a line by selecting a voice mail profile.
- Cisco Unity integration with Cisco Unified Communications Manager is configured using the Cisco Unity Telephony Integration Manager (UTIM).
- Subscribers have to be added in Cisco Unity.

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Release 5.0 – Setting Up a Cisco Unified Communications Manager 6.0 SCCP Integration with Cisco Unity
http://www.cisco.com/en/US/docs/voice_ip_comm/unity/5x/integration/cucm_sccp/guide/cuintcucmskinny080.html

Lesson 5

Implementing Cisco Unified Video Advantage

Overview

Cisco Unified Video Advantage is a video telephony solution comprising the Cisco Unified Video Advantage software and Cisco Video Telephony (VT) Camera, a Universal Serial Bus (USB) camera. With the Cisco VT Camera attached to a PC collocated with a Cisco IP phone, users can place and receive video calls on the enterprise IP telephony network. Customers can take full advantage of their IP networks to deliver enterprise-class business communications that extend voice and video to every user in the organization.

Objectives

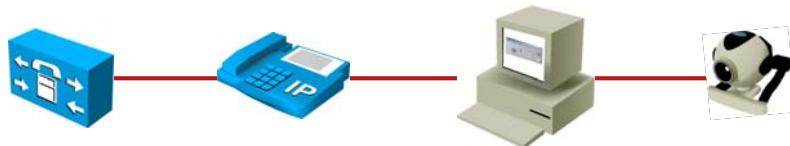
Upon completing this lesson, you will be able to configure Cisco Unified Video Advantage and Cisco Unified Communications Manager to make video telephony calls. This ability includes being able to meet these objectives:

- Describe Cisco Unified Video Advantage
- Describe the protocols used between the components of Cisco Unified Video Advantage
- Describe how to configure Cisco Unified Communications Manager to support Cisco Unified Video Advantage
- Describe how to install Cisco Unified Video Advantage on a PC
- Describe how to verify and diagnose Cisco Unified Video Advantage operation on a PC

Cisco Unified Video Advantage Overview

This topic describes Cisco Unified Video Advantage.

Cisco Unified Video Advantage Overview



- Cisco Unified Video Advantage adds video capabilities to an IP phone.
- It uses software on a PC connected to an IP phone.
- The PC has a video camera connected.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-4

Cisco Unified Video Advantage brings video telephony functionality to the Cisco Unified IP Phones 794[0125], 796[0125], and 797[015] models. Cisco Unified Video Advantage software coupled with the Cisco VT Camera (a USB camera) allows a PC connected to a Cisco IP phone to add video to telephone calls without requiring any extra button-pushing or mouse-clicking. When registered to Cisco Unified Communications Manager, the Cisco IP phone enabled with Cisco Unified Video Advantage has the features and functionality of a full-featured IP video phone. Supplementary services, such as call forward, transfer, hold, and mute, are also available for video calls, and are all initiated through the Cisco IP phone. Cisco Unified Video Advantage is intended for desktop-to-desktop IP video telephony environments, not as a general-purpose videoconferencing solution for use in conference rooms.

Cisco Unified Video Advantage Components

The figure shows the components of a Cisco Unified Video Advantage implementation.

Cisco Unified Video Advantage Components

- Unified CM:
 - Release 4.0(1) with Service Release 2 or later
- Cisco Unified IP Phones 794[0125], 796[0125], or 797[015] (or alternatively Cisco IP Communicator 2.0 or later)
- PC with video camera and software:
 - Cisco Unified Video Advantage camera connected via USB
 - Cisco Unified Video Advantage software



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-5

To deploy Cisco Unified Video Advantage, the minimum requirement is Cisco Unified Communications Manager Release 4.0(1) with Service Release 2 or later.

Currently, video can be enabled on Cisco Unified IP Phones 794[0125], 796[0125], and 797[015] models. The Cisco VT Camera is connected to a PC (via USB) where Cisco Unified Video Advantage software is installed. Cisco Unified Video Advantage software works only with the Cisco VT Camera.

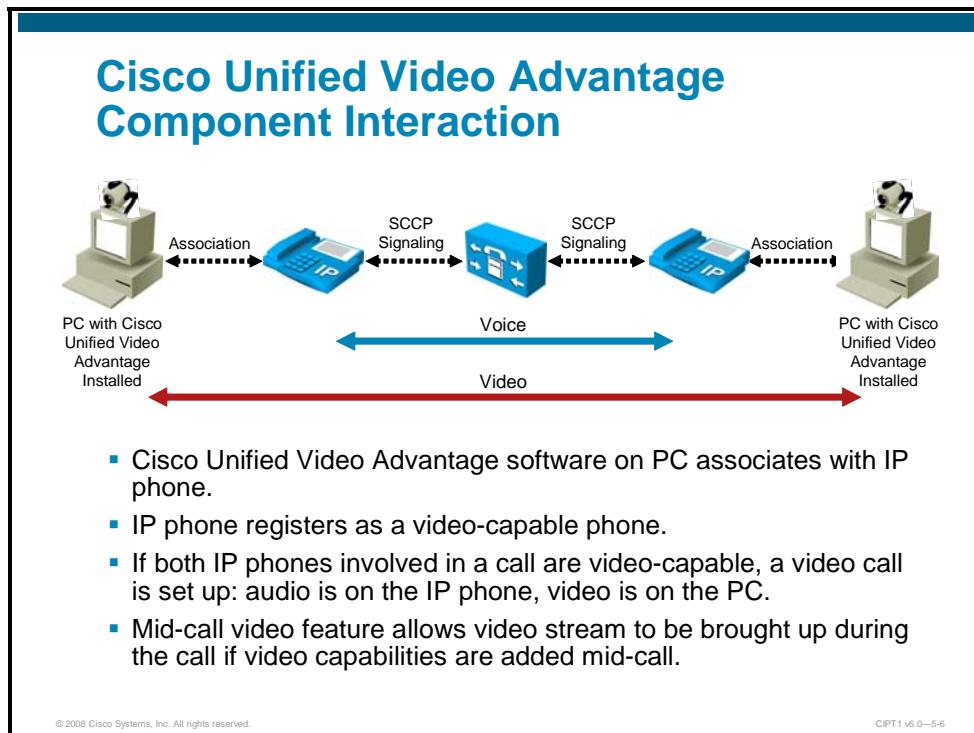
Note	When using Cisco IP Communicator 2.0 or later and Cisco Unified Video Advantage 2.0 or later, Cisco Unified Video Advantage can interact with Cisco IP Communicator rather than a Cisco IP phone. Cisco Unified Video Advantage and Cisco IP Communicator must run on the same PC in this case.
-------------	---

Cisco Unified Video Advantage software provides the user with an easy-to-use graphical interface, including these options:

- **Camera On:** Users can turn the camera on and off.
- **Video Check:** Users can check their video before calls are placed or received.
- **Mute Video on Audio Mute:** When users mute the audio on the IP phone, video is automatically paused until the audio on the IP phone is restored.
- **Video Signal Indicators:** The quality of the incoming and outgoing video is graphically displayed.
- **Connectivity Indicator:** Graphics are used to indicate the state of the connection from the PC to its associated Cisco IP phone or Cisco IP Communicator.

Cisco Unified Video Advantage Component Interaction

The figure illustrates the component interaction when using Cisco Unified Video Advantage.



The Cisco Unified Video Advantage software is running on the PC connected directly to the PC access port on the back of the Cisco IP phone.

The PC and the Cisco IP phone build an association. After that the IP phone registers its video capabilities with Cisco Unified Communications Manager.

If a call is placed between two video-capable IP phones, the call is set up as a video call in which audio is on the IP phone and video is on the PC.

The mid-call video feature allows the video stream to be brought up at any time during the call, as soon as video capabilities are added to the phone (that is, when Cisco Unified Video Advantage is started on the PC).

Cisco Unified Video Advantage Supported Multimedia Standards

The figure shows the video codecs that Cisco Unified Video Advantage supports.

Cisco Unified Video Advantage Supported Multimedia Standards

- H.263 and H.264 video codec (from 50 kbps to 1.5 Mbps)
- Cisco wideband video codecs (7 Mbps)
- Supports video formats up to 30 fps:
 - CIF (352 x 288, 230 x 240)
 - QCIF (176 x 144, 160 x 120)

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-7

Cisco Unified Video Advantage supports three types of video codecs: H.263, H.264, and the Cisco wideband video codec. Of these types, the Cisco wideband video codec places the least demand on the PC. Therefore, if your network has sufficient available bandwidth, you can use the Cisco wideband video codec and save on PC, CPU, and memory resources.

When you use a codec that must be compressed, more CPU power is needed. The H.263 and the H.264 codecs are more demanding of PC system resources, but they require less bandwidth. Therefore, if you want to use H.263 or H.264 compressed video to conserve bandwidth on the network, you should ensure that your PCs have enough CPU and memory resources available. The Cisco Unified Video Advantage H.263 and H.264 codecs support a bandwidth range from 50 kbps to 1.5 Mbps.

In summary, you must balance PC performance with network utilization when deploying Cisco Unified Video Advantage.

Cisco Unified Video Advantage Communication Flows

This topic describes communication flows when you use Cisco Unified Video Advantage, and describes the protocols that are used between Cisco Unified Video Advantage components.

Protocols Used by Cisco Unified Video Advantage

- Cisco Discovery Protocol: Discovery between IP phone and PC
- Cisco Audio Session Tunnel: Association and signaling between IP phone and Cisco Unified Video Advantage software
- SCCP: Signaling between IP phone and Unified CM
- RTP: Media transport (video to Cisco Unified Video Advantage, audio to phone)

Cisco Unified Video Advantage supports several industry-standard and Cisco networking protocols required for video communications, as shown in the table.

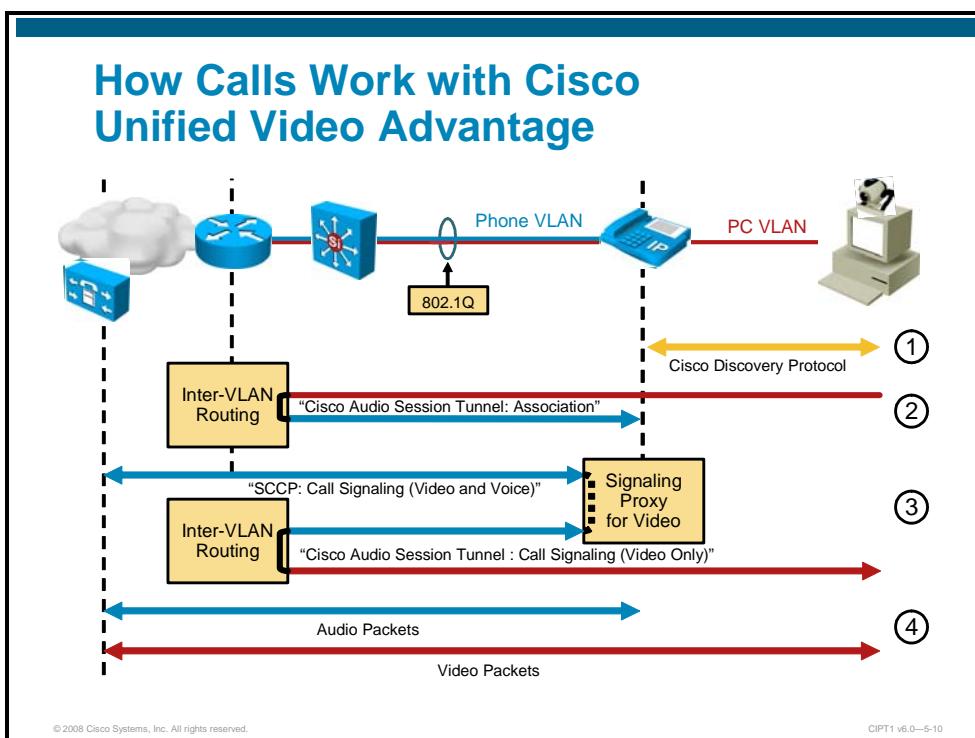
Protocols Used by Cisco Unified Video Advantage

Networking Protocol	Description	Usage Notes
Cisco Audio Session Tunnel	<ul style="list-style-type: none"> ■ Allows communication between the Cisco IP phone and associated software, such as Cisco Unified Video Advantage ■ Uses source and destination TCP port 4224 ■ Uses TCP ■ Cisco proprietary protocol 	<ul style="list-style-type: none"> ■ Cisco Audio Session Tunnel is used between Cisco Unified Video Advantage and the IP phone for these tasks: <ul style="list-style-type: none"> — To build an association (after the PC discovers the IP phone, using Cisco Discovery Protocol) — To send signaling information for video streams from the IP phone to Cisco Unified Video Advantage (after the IP phone receives the signaling messages for both audio and video from Cisco Unified Communications Manager) ■ Cisco Audio Session Tunnel signaling messages include the following: <ul style="list-style-type: none"> — Call video stream start and stop — Call hold and resume
Cisco Discovery Protocol	<ul style="list-style-type: none"> ■ A device-discovery protocol that runs on all Cisco manufactured equipment ■ A Layer 2 protocol ■ Works only between directly connected neighbors ■ Using Cisco Discovery Protocol, a device can advertise its existence to other devices and receive information about other devices in the network ■ A Cisco proprietary protocol 	<ul style="list-style-type: none"> ■ Cisco Unified Video Advantage uses Cisco Discovery Protocol to communicate its capabilities to the Cisco IP phone, and the Cisco IP phone uses Cisco Discovery Protocol to communicate information, such as its IP address, to Cisco Unified Video Advantage.
Real-Time Transport Protocol (RTP)	<ul style="list-style-type: none"> ■ A standard for using User Datagram Protocol (UDP) to transport real-time data, such as interactive voice and video, over data networks 	<ul style="list-style-type: none"> ■ RTP is used to encapsulate and stream the audio (between Cisco IP phones) and video (between Cisco Unified Video Advantage endpoints).
Skinny Client Control Protocol (SCCP)	<ul style="list-style-type: none"> ■ A Cisco protocol using low-bandwidth messages, which allows the exchange of signaling messages between IP devices and the Cisco Unified Communications Manager ■ Works on TCP port 2000 ■ A Cisco proprietary protocol 	<ul style="list-style-type: none"> ■ Cisco Unified Video Advantage does not use SCCP itself. It uses Cisco Audio Session Tunnel to send signaling messages to the Cisco IP phone, which acts as a proxy and passes the signaling messages to Cisco Unified Communications Manager using SCCP.

Note	On Cisco Unified IP Phones 794[125], 796[125], and 797[015], SIP can be used instead of SCCP. The Cisco Unified IP Phones 7940 and 7960 only support Cisco Unified Video Advantage if using SCCP.
-------------	---

How Calls Work with Cisco Unified Video Advantage

This subtopic describes how calls work when you are using Cisco Unified Video Advantage.



When a Windows PC has Cisco Unified Video Advantage installed, it should be connected to the secondary Ethernet port (that is, PC port) of a Cisco Unified IP Phone 794[0125], 796[0125], or 797[015] model. In most configurations, the PC will be in a different VLAN (the access or native VLAN) from the Cisco IP phone (located in the voice or auxiliary VLAN). In such configurations, all IP-based communication between Cisco Unified Video Advantage and the Cisco IP phone must be routed between the VLANs, and only Cisco Discovery Protocol is exchanged directly. Cisco Unified Video Advantage works as follows:

- Step 1** Cisco Discovery Protocol exchange takes place so that Cisco Unified Video Advantage and the Cisco IP phone can discover each other. A Cisco Discovery Protocol driver is installed on the PC during the installation of Cisco Unified Video Advantage. This driver allows the Cisco Unified Video Advantage application to dynamically learn the IP address of the Cisco IP phone during the Cisco Discovery Protocol exchange, and associate with it. This feature provides both ease of use for the end user and security. The use of Cisco Discovery Protocol to facilitate the association allows the process to occur automatically, without the user having to configure the Cisco Unified Video Advantage application. This feature allows mobility of the application between different IP phones on the network. The user may connect a PC to the PC port of any supported Cisco IP phone on the network (if permitted by the administrator and if the IP phone has video enabled) and begin making video telephony calls. Cisco Discovery Protocol also provides a measure of security because the IP phone will respond only to association messages from a Cisco Unified Video Advantage client that matches the IP address of the device that is connected to its PC port (that is, its Cisco Discovery Protocol neighbor), minimizing the risk of someone else associating with your Cisco IP phone over the network and receiving video when calls are placed on your IP phone. The Cisco IP phone begins listening for Cisco Audio Session Tunnel messages on TCP port 4224.

- Step 2** After Cisco Discovery Protocol discovery, Cisco Unified Video Advantage and the IP phone exchange Cisco Audio Session Tunnel protocol messages over TCP/IP. Cisco Unified Video Advantage sends a Cisco Audio Session Tunnel message to the IP phone, which is in a different IP network (that is, different VLAN). The packet first travels through the PC VLAN to the default gateway, where it is routed toward the IP phone (using the voice VLAN). The Cisco Audio Session Tunnel protocol allows Cisco Unified Video Advantage to associate with the IP phone and receive event messages from the IP phone when calls are placed or received. After this association process occurs between the Cisco Unified Video Advantage client and the IP phone, the IP phone updates its registration status with Cisco Unified Communications Manager, advising Cisco Unified Communications Manager of its video capabilities.
- Step 3** When the Cisco IP phone receives signaling information for video calls, it acts as a proxy toward Cisco Unified Video Advantage for the setup of the video streams. Only the signaling is proxied, but when the RTP endpoints (IP addresses and UDP RTP port numbers) are negotiated, the IP phone specifies the IP address of the PC for the video stream and its own IP address for the audio stream. When Cisco Unified Communications Manager tells the Cisco IP phone to open the video channel, (communicating to the IP phone using the voice VLAN) the IP phone proxies those messages to Cisco Unified Video Advantage using Cisco Audio Session Tunnel protocol. These Cisco Audio Session Tunnel messages must be routed between the voice and the PC VLAN again.
- Step 4** After the voice and video channels have been successfully set up, the audio stream is sent to the IP address of the IP phone (to the voice VLAN) while the video stream is sent directly to the PC IP address (to the PC VLAN).

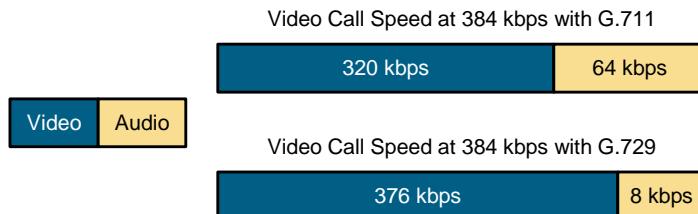
Note Firewalls or access control lists (ACLs) must permit TCP port 4224 from the data VLAN to the voice VLAN in order to allow the exchange of Cisco Audio Session Tunnel messages.

Video Call Bandwidth for Audio and Video Channels

This subtopic describes the bandwidth that is used for audio and video channels of a video call.

Video Call Bandwidth for Audio and Video Channels

- Video call includes two channels:
 - Audio channel
 - Video channel
- The bit rate available for the video channel depends on the negotiated audio codec and the overall video call speed.



© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-11

A typical video call consists of two media channels: one for the video stream and one for the audio stream.

The audio channel consists of the actual audio bit rate. This bit rate is dictated by the audio codec in use. In the case of a G.711 codec, the bit rate is 64 kbps, while in the case of a G.729 codec, it is 8 kbps. For an audio channel, only the pure audio data is considered, not the packetization overhead.

The bit rate available for the video channel depends on the negotiated audio codec and the video call speed. The video channel bit rate is the speed of the video call minus the bit rate of the codec used for the audio channel. In the case of a 384-kbps video call with an audio channel that uses G.711, the bit rate left for the video channel is 320 kbps (384 kbps minus 64 kbps). In the case of an audio channel using the G.729 codec, the payload of the same video call (384 kbps) leaves 376 kbps for the video channel (384 kbps minus 8 kbps).

This table lists examples of video call speeds, audio channel codecs, and the associated video channel bit rates.

Video Call Speeds and the Associated Audio and Video Codecs

Video Call Speed	Audio Codec and Rate	Video Codec and Rate
128 kbps	G.711 at 64 kbps	H.261 or H.263 at 64 kbps
128 kbps	G.729 at 8 kbps	H.261 or H.263 at 120 kbps
128 kbps	G.728 at 16 kbps	H.261 or H.263 at 112 kbps
384 kbps	G.729 at 8 kbps	H.261 or H.263 at 376 kbps
384 kbps	G.711 at 64 kbps	H.261 or H.263 at 320 kbps

Video Call Speed	Audio Codec and Rate	Video Codec and Rate
768 kbps	G.729 at 8 kbps	H.261 or H.263 at 760 kbps
768 kbps	G.711 at 64 kbps	H.261 or H.263 at 704 kbps
1.472 Mbps	G.729 at 8 kbps	H.261 or H.263 at 1.464 Mbps
1.472 Mbps	G.711 at 64 kbps	H.261 or H.263 at 1.408 Mbps
7 Mbps	G.729 at 8 kbps	Wideband at 7 Mbps (minus 8 kbps for the audio stream)
7 Mbps	G.711 at 64 kbps	Wideband at 7 Mbps (minus 64 kbps for the audio stream)

Cisco Unified Video Advantage Configuration in Cisco Unified Communications Manager

This topic describes how to configure Cisco Unified Communications Manager to support Cisco Unified Video Advantage.

Unified CM Cisco Unified Video Advantage Configuration Procedure

1. Configure regions with the maximum audio codec and video call speed to be used per video call.
2. Configure the maximum allowed bandwidth used by video calls between different locations.
3. Configure the IP phone in Unified CM to support Cisco Unified Video Advantage.
4. Verify Cisco Unified Video Advantage support on the IP phone.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-13

Cisco Unified Video Advantage configuration in Cisco Unified Communications Manager includes the following steps:

- Step 1** Configure regions with the maximum audio codec and video call speed to be used per video call.
- Step 2** Configure the maximum allowed bandwidth used by video calls within or between locations.
- Step 3** Configure the IP phone in Cisco Unified Communications Manager to support Cisco Unified Video Advantage.
- Step 4** Verify Cisco Unified Video Advantage support on the IP phone.

Step 1: Setting the Maximum Audio Codec and Video Call Speed Allowed Per Video Call

This subtopic describes how to configure the maximum audio codec and video call speed to be used by a Cisco Unified Video Advantage call.

The screenshot shows the 'Region Configuration' screen with the following details:

- Region Information:** Name is set to 'Default'.
- Region Relationships:** Default region has 'Audio Codec' set to 'G.711' and 'Video Call Bandwidth' set to '384'. A note says 'NOTE: Regions(s) not displayed'.
- Modify Relationship to other Regions:** Default region has 'Audio Codec' set to 'G.711' and 'Video Call Bandwidth' set to '384 kbps'.

Callouts provide additional information:

- A callout for the 'Audio Codec' field states: "Sets audio codec with the highest allowed codec bit rate. Applies to audio channels of audio and video calls."
- A callout for the 'Video Call Bandwidth' field states: "Sets the maximum video call speed. Includes audio and video channel."

At the bottom left is the copyright notice: © 2008 Cisco Systems, Inc. All rights reserved. At the bottom right is the document identifier: CIPT1 v6.0—5-14.

The audio codec and video call speed settings are configured under **System > Region**.

Note that the audio setting specifies a codec type, while the video setting specifies the bandwidth that you want to allow. However, even though the notation is different, the Audio Codec and Video Call Bandwidth fields actually perform similar functions. The Audio Codec value defines the maximum bit rate allowed for audio-only calls and for the audio channel in video calls.

For instance, if you set the Audio Codec value for a region to G.711, Cisco Unified Communications Manager allocates 64 kbps as the maximum bandwidth allowed for the audio channel for that region. In this case, Cisco Unified Communications Manager permits calls using G.711, G.728, or G.729. However, if you set the Audio Codec value to G.729, Cisco Unified Communications Manager allocates only 8 kbps as the maximum bandwidth allowed for the audio channel; in addition, Cisco Unified Communications Manager permits calls using only G.729, because G.711, G.722, and G.728 all require more than 8 kbps.

The Video Call Bandwidth value defines the maximum bit rate for the video call, that is, the bit rate of the voice and video channels. For instance, if you want to allow video calls at a speed of 384 kbps using G.711 audio, you would set the Video Call Bandwidth value to 384 kbps and the Audio Codec value to G.711. The bit rate that would be used by the video channel thus would be 320 kbps.

If the Video Bandwidth value is set to None for the region, Cisco Unified Communications Manager either terminates the call or allows it to pass as an audio-only call, depending on whether the called device has the Retry Video Call as Audio option enabled.

In summary, the Audio Codec field defines the maximum bit rate used for the audio channel of audio-only calls and for the audio channel of video calls, while the Video Call Bandwidth field defines the maximum bit rate allowed for video calls and includes the audio portion of the video call.

Step 2: Setting the Maximum Allowed Bandwidth Used by Video Calls for Locations

This section describes how to configure the maximum total bandwidth that can be consumed by video calls between different locations.

Step 2: Setting the Maximum Allowed Bandwidth Used by Video Calls for Locations

System > Location

Location Configuration

Related Links: [Back To Find>List](#) [Go](#)

Location Information

Name * Hub_None

Audio Calls Information

Audio Bandwidth * Unlimited kbps

If the audio quality is poor or choppy, lower the bandwidth setting. For ISDN, use multiple kbps or 64 kbps.

Video Calls Information

Video Bandwidth * None Unlimited kbps

Sets the maximum audio bandwidth for a location.
Applies to audio-only calls only, not to audio channel of a video call.

Sets the maximum video bandwidth for a location.
Applies to audio and video channels of video calls.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-15

When configuring locations, you also set two fields in Cisco Unified Communications Manager Administration: the Audio Bandwidth and the Video Bandwidth values. Locations are configured under **System > Location**.

Unlike the settings for regions, however, audio bandwidth for locations applies only to audio-only calls, while video bandwidth again applies to the video call (that is, audio and video channels).

Note

The audio and video bandwidth are kept separate, because if both types of calls shared a single allocation of bandwidth, it is very likely that audio calls would take all of the available bandwidth and leave no room for any video calls, or vice versa.

Both the Audio Bandwidth and the Video Bandwidth fields offer the options of Unlimited and a numeric value, while Video Bandwidth can also be set to None, in which case video calls are not allowed between this location and other locations. Video calls can, however, be placed within this location. The Unlimited option lifts any bandwidth restrictions. If numeric values are configured, they use two different calculation models, as follows:

- For the Audio Bandwidth field, the value entered must include the Layer 3 overhead required for the call. For instance, if you want to permit a single G.729 call to or from a location, you would enter the value 24 kbps. For a G.711 call, you would enter the value 80 kbps. The payload of a G.711 voice call is 64 kbps; the 80-kbps value is the 64-kbps payload plus 16-kbps RTP plus UDP plus IP overhead.

- The value in the Video Bandwidth field, by contrast, is entered without any overhead. For instance, for a 128-kbps call, enter the value 128 kbps; for a 384-kbps call, enter the value 384 kbps. As with the values used in the Video Bandwidth field for regions, it is recommended that you always use increments of 56 kbps or 64 kbps for the Video Bandwidth field for locations.

If you use Resource Reservation Protocol (RSVP) for Call Admission Control (CAC) between locations, then for each other location you have to set the RSVP setting to one of the following:

- **Use System Default:** The RSVP policy to the selected location matches the Cisco Unified Communications Manager Default Interlocation RSVP Policy service parameter. The default value for this service parameter is No Reservation.
- **No Reservation:** No RSVP reservations are made to the selected location.
- **Optional (Video Desired):** A call can proceed as a best-effort audio-only call if no reservations for both the audio and video streams can be obtained. Cisco RSVP Agent continues to attempt RSVP reservation and informs Cisco Unified Communications Manager if reservation succeeds.
- **Mandatory:** Cisco Unified Communications Manager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream as well.
- **Mandatory (Video Desired):** A video call can proceed as an audio-only call if a reservation for the video stream cannot be obtained.

The default value for the RSVP setting is to use the system default.

Note	More information about CAC using locations and RSVP-enabled locations is provided in the CIPT2 course.
-------------	--

Step 3: Required Phone Configuration Settings for Video Support

This subtopic describes how to configure a Cisco IP phone in Cisco Unified Communications Manager to support Cisco Unified Video Advantage.

Step 3: Required Phone Configuration Settings for Video Support

Device > Phone

Product Specific Configuration

<input type="checkbox"/> Disable Speakerphone	<input type="checkbox"/> Disable Speakerphone and Headset
PC Port *	<input checked="" type="text" value="Enabled"/>
Settings Access *	<input checked="" type="text" value="Enabled"/>
Gratuitous ARP *	<input checked="" type="text" value="Enabled"/>
PC Voice VLAN Access *	<input checked="" type="text" value="Enabled"/>
Video Capabilities *	<input checked="" type="text" value="Enabled"/>
Auto Line Select *	<input type="text" value="Disabled"/>
Web Access *	<input checked="" type="text" value="Enabled"/>

PC Port (enabled by default): Must be enabled.

Video Capabilities (disabled by default): Must be enabled.

© 2008 Cisco Systems, Inc. All rights reserved. CIPT1 v6.0—5-16

The IP phone configuration settings that are required for video support can be found in the IP phone configuration window of Cisco Unified Communications Manager Administration (Go to **Device > Phone**).

The IP phone settings need not be configured before Cisco Unified Video Advantage can be loaded on the client PC. But the preferred sequence is to configure the IP phone first and then install the Cisco Unified Video Advantage software, as follows:

- Because the PC that has Cisco Unified Video Advantage installed needs to be physically connected to a PC port of the IP phone, you must ensure that the PC port of the IP phone is not disabled under the Cisco Unified Communications Manager IP phone configuration. By default, the PC port is enabled.
- When the Video Capabilities field is set to Enabled, the phone will participate in video calls when connected to an appropriately equipped PC. Make sure that this feature is enabled on Cisco IP phones that operate with Cisco Unified Video Advantage. Video capability is disabled by default.

The Retry Video Call as Audio check box is located in the Phone Configuration window, and this feature is activated by default. If you uncheck this check box, a video call that fails to connect is not attempted as an audio-only call instead.

Step 4: Verification of Phone Configuration

This subtopic describes how to verify IP phone configuration.

Step 4: Verification of Phone Configuration



- A video-enabled IP phone shows a small camera on its screen.
- The symbol is visible after the phone is configured to support video calls:
 - It does not indicate that Cisco Unified Video Advantage has been associated with the IP phone.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-17

An IP phone enabled for video displays a video camera icon in the lower right corner of its LCD screen.

A PC with Cisco Unified Video Advantage installed does not have to be connected to the IP phone to produce the video camera icon. The camera icon is displayed as soon as video is enabled for the IP phone in Cisco Unified Communications Manager configuration. It does not indicate a successful association of the Cisco Unified Video Advantage software running on the PC and the IP phone.

Cisco Unified Video Advantage Installation

This topic describes how to install the Cisco Unified Video Advantage software on a PC.

Cisco Unified Video Advantage Installation Procedure

1. Consider hardware requirements
2. Consider software requirements
3. Install Cisco Unified Video Advantage software and hardware

©2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-19

Cisco Unified Video Advantage installation includes the following steps:

Step 1 Consider hardware requirements

Step 2 Consider software requirements

Step 3 Install Cisco Unified Video Advantage software and hardware

Step 1: Cisco Unified Video Advantage Hardware Requirements

This subtopic describes the hardware requirements for Cisco Unified Video Advantage.

Step 1: Cisco Unified Video Advantage Hardware Requirements

- PC:
 - At least 1.9 GHz CPU
 - At least 512 MB memory
 - At least 100 MB free disk space
 - At least one USB port
 - Connected to a Cisco Unified IP Phone 794[0125], 796[0125], or 797[015] or colocated with Cisco IP Communicator
- Cisco VT Camera:
 - Connected to a USB port of the PC

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-20

The hardware requirements are as follows:

- Compatible Cisco IP phone or Cisco IP Communicator
- PC
- Cisco VT Camera

Cisco IP Phone

Cisco Unified Video Advantage is supported on the Cisco Unified IP Phone 794[0125], 796[0125], and 797[015] models and on Cisco IP Communicator.

PC Hardware Requirements

The table describes the hardware requirements for the PC when Cisco Unified Video Advantage software is used with Cisco IP phones.

Hardware Requirements for the PC When Cisco Unified Video Advantage Software Is Used with Cisco IP Phones

PC Feature	Minimum Requirements
CPU	<ul style="list-style-type: none">■ Cisco Unified Video Advantage using H.263<ul style="list-style-type: none">— 1.9 GHz or higher Pentium IV or compatible processor (Streaming Single Instruction, Multiple Data (SIMD) Extensions support required)■ Cisco Unified Video Advantage using H.264<ul style="list-style-type: none">— 2.4 GHz or higher Pentium IV or compatible processor (Streaming SIMD Extensions support required)■ 2.8 GHz or higher compatible processor recommended
System memory	512 MB minimum, 1 GB recommended
Free disk space	At least 100 MB, 200 MB when being used with Cisco IP Communicator
USB port	At least one free USB (1.1- or 2.0-compliant) port, version 2.0 recommended
Video display	Minimum: DirectX 9.0 compatible graphics card with 32 MB of Video RAM, for dual-headed configurations, 64 MB Recommended: DirectX 9.0 compatible graphics card with 64 MB of Video RAM, for dual-headed configurations, 128 MB
Network	10/100 Ethernet network interface card (NIC)

Cisco VT Camera

The Cisco VT Camera must be connected to the PC during the installation of the Cisco Unified Video Advantage software on the PC.

Note Cisco Unified Video Advantage supports only the Cisco VT Camera, and the Cisco VT Camera works only with the Cisco Unified Video Advantage software.

Before the introduction of Cisco Unified Communications Manager Release 5.0, Cisco Unified Video Advantage was known as Cisco VT Advantage. With this change, not only the software but also the camera was updated. The Cisco VT Camera that was used with the Cisco VT Advantage solution reached end-of-sale status on May 24, 2006. It is replaced by the Cisco VT Camera II, which began shipping in June 2006.

The difference between Cisco VT Camera II and Cisco VT Camera is not functional and does not affect the functionality of Cisco Unified Video Advantage. Existing Cisco VT Advantage users do not have to replace their cameras with Cisco VT Camera II. Cisco VT Camera II requires the use of Cisco Unified Video Advantage software version 2.0(1) or later. This software version will support both Cisco VT Camera and Cisco VT Camera II.

Step 2: Cisco Unified Video Advantage Software Requirements

This section describes the software requirements for Cisco Unified Video Advantage.

Step 2: Cisco Unified Video Advantage Software Requirements

- Operating system:
 - MS Windows 2000 with Service Pack 4 or later
 - MS Windows XP with Service Pack 2 or later
- Cisco Unified Video Advantage software
 - Downloaded from Cisco.com

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-21

The Cisco Unified Video Advantage software must be installed on the PC connected directly to the Cisco IP phone or running Cisco IP Communicator.

PC Feature Requirements

The minimum requirement for the operating system of the PC is either Microsoft Windows 2000 Professional with Service Pack 4 or later, or Microsoft Windows XP Professional with Service Pack 2 or later.

Cisco Unified Video Advantage Software

You can download the Cisco Unified Video Advantage software from <http://www.cisco.com> and then distribute it to the corresponding PCs.

Step 3a: Cisco Unified Video Advantage Installation – Preparation Checklist

Follow the installation preparation checklist before starting the installation of the Cisco Unified Video Advantage software on the PC.

Step 3a: Cisco Unified Video Advantage Installation – Preparation Checklist

- Ensure that the Cisco IP phone or Cisco IP Communicator is registered.
- Ensure that the Cisco IP phone or Cisco IP Communicator is video-enabled.
- Ensure that the PC is connected to the IP phone and verify IP connectivity between IP phone and PC (not needed with Cisco IP Communicator):
 - Check reachability using ping
 - Ensure that Cisco Audio Session Tunnel protocol is not filtered between PC and IP phone

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-22

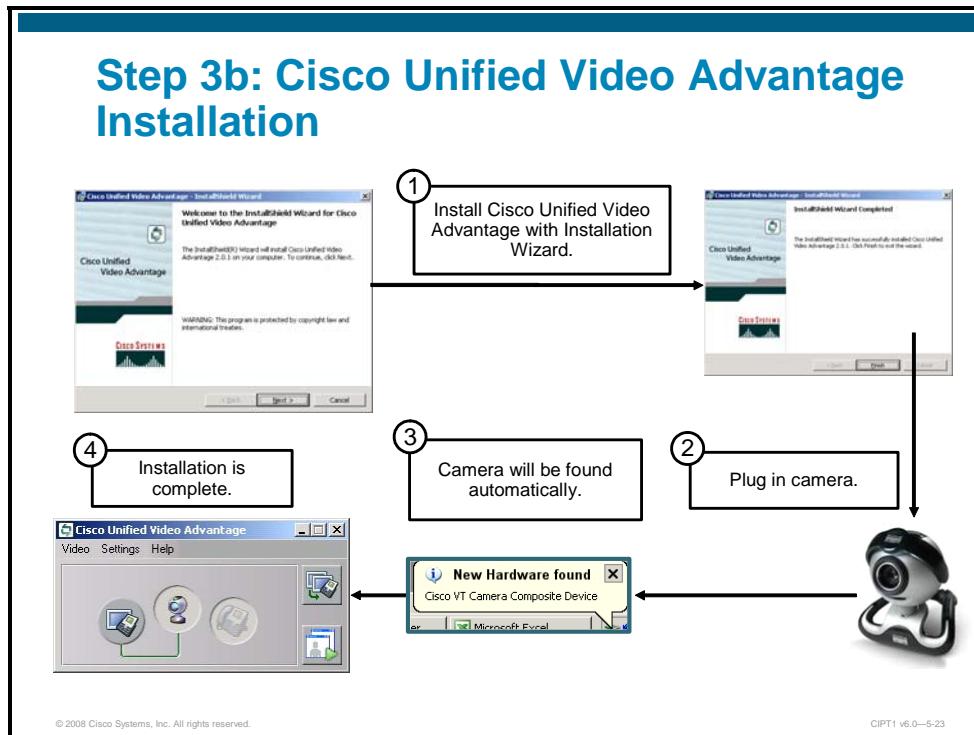
The items to be checked before starting the installation are as follows:

- Ensure that the Cisco IP phone or Cisco IP Communicator is properly connected to the corporate telephony network and successfully registered with Cisco Unified Communications Manager. You could do a short audio test call to ensure that the IP phone is working correctly.
- Ensure that the Cisco IP phone or Cisco IP Communicator is video-enabled. If the LCD screen on the Cisco IP phone displays the video camera icon on the status line, the phone is video-enabled.
- Ensure that the Ethernet port of the PC is connected to the PC port of the IP phone, because this connection is mandatory for Cisco Unified Video Advantage (unless using Cisco IP Communicator).
- For the Cisco Audio Session Tunnel protocol to operate between Cisco Unified Video Advantage and the IP phone, the PC must be capable of reaching the IP phone over TCP/IP port 4224. Typical IP telephony designs use separate voice and data VLANs, as well as ACLs or firewalls between those VLANs, to secure the IP telephony network.

Note	When using Cisco IP Communicator, you must ensure that Cisco Audio Session Tunnel can be used between the Cisco Unified Video Advantage application and Cisco IP Communicator. A host-based intrusion prevention system or personal firewall might block this communication by default.
-------------	---

Step 3b: Cisco Unified Video Advantage Installation

After you have verified all hardware and software requirements and completed the preparation checklist, you can install Cisco Unified Video Advantage.



Launch the installation file and complete these steps:

- Step 1** Make sure that the Cisco VT Camera is *not* connected to the PC.
- Step 2** Follow the instructions in the dialog boxes that appear to complete the installation of Cisco Unified Video Advantage:
- In the Welcome window, click **Next** to start the installation wizard.
 - In the License Agreement window, click **I Accept the Terms in the License Agreement**, and click **Next**.
 - In the Destination Folder window, accept the default installation folder or click **Change** to enter a different installation folder. When you are done, click **Next**.
 - In the Ready to Install the Program window, click **Install** and wait until you see the Shortcut Options window. Depending on the setup of your PC and the operating system that you use, there might be additional windows or messages that require your attention before you get to the Shortcut Options window.
 - In the Shortcut Options window, make your choices about icons to be added to the quick-launch bar or to the desktop. You can also choose whether you want Cisco Unified Video Advantage to be started automatically at system startup. Click **Next** when you have made your selection.
 - A window appears indicating that the installation has been completed. Confirm the message by clicking **Finish**.
 - If you are prompted to restart the PC, click **Yes** to restart the PC.

- Step 3** After installation has finished and PC has been rebooted, you can plug in the camera. All necessary drivers are installed so that the new device should be correctly identified and added to the system.
- Step 4** After the new hardware has been added, Cisco Unified Video Advantage is ready to be used.

Cisco Unified Video Advantage Verification Tools

This topic describes verification and diagnostic tools of Cisco Unified Video Advantage.

Cisco Unified Video Advantage Verification of IP Phone Association

- After starting the Cisco Unified Video Advantage software, verify the status of the connection to the IP phone or Cisco IP Communicator.



Camera Associated with
Cisco IP Communicator,
Connection Successful



Camera Associated with
IP Phone, Connection
Not Successful

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-25

You can verify the association of Cisco Unified Video Advantage and the IP phone or Cisco IP Communicator from the status displayed on the application window.

When the Cisco Unified Video Advantage application is started, it will show icons for the Cisco VT Camera in the middle, Cisco IP Communicator on the left, and an IP phone on the right. You can click Cisco IP Communicator or the IP phone icon to instruct Cisco Unified Video Advantage with which device it should associate. A successful connection is indicated by a green line, while an unsuccessful connection is indicated by a broken red line.

Cisco Unified Video Advantage Verification of Camera

After you ensure that the camera has successfully associated with a phone (either an IP phone or Cisco IP Communicator), you should run a video check.

Cisco Unified Video Advantage Verification of Camera

- After verifying the camera connection status, run a video check, and you should see the camera input in both windows, the remote and the local view.



To start the video check, choose **Video > Start Video Check** or simply click the button in the bottom left corner of the Cisco Unified Video Advantage application window. While the video check is being performed, two popup windows show the local view and remote view. Inside the windows, green bars are displayed (one for the sending video signal and the other for the receiving video signal). During the video check, you will see the same image in both windows.

Active Call Verification with the Diagnostic Tool

This subtopic describes the diagnostic tool of Cisco Unified Video Advantage.

Active Call Verification with the Diagnostic Tool

- You can open a call diagnostic window by right-double-clicking the Cisco Unified Video Advantage application window.
- The diagnostic window allows you to monitor Cisco Discovery Protocol packets, Cisco Audio Session Tunnel packets, and active call statistics.

The screenshot shows the Cisco Diagnostics interface with three main windows:

- CAST Messages:** Displays log entries such as "02-08-30-078 SEND StatusUpdate Capabilities Cisco IP Communicator H.263 Resolution=CCIF/CP" and "02-08-07-169 3047 StatusUpdate Capabilities Cisco IP Communicator H.263 Resolution=CCIF/CP".
- Discovery Messages:** Displays log entries for discovered IP Communicators, including their IP address (e.g., 192.168.201.53), port (e.g., 4225), and protocol (e.g., CDP).
- Video Check Information:** A split-screen window showing "Transmit" and "Receive" details for a video call. Both sides show H.263 as the Codec, 3500000 as the Call Bitrate, CIF as the Resolution, and LOOPBACK as the IP Address. Port 5445 is listed for both sides. Frame Rate is 25 for both. Total frames sent/received are 248, and total partial frames are 0. Frame errors are 0 for both.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-27

While in the call, you can launch the diagnostic tool. The diagnostic tool provides some technical details about the current state of the Cisco Unified Video Advantage software that is running on the PC, as well as some indications about the Cisco VT Camera frame rates and errors.

To use the diagnostic tool, open the Cisco Unified Video Advantage main window and double-right-click the application window. The Diagnostics window appears.

The diagnostic tool allows monitoring of Cisco Discovery Protocol messages, Cisco Audio Session Tunnel packets, and active call statistics.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco Unified Video Advantage adds video capabilities to Cisco IP phones by using software and camera on a PC attached to the IP phone.
- Cisco Unified Video Advantage discovers the IP phone by listening to Cisco Discovery Protocol messages and uses the Cisco Audio Session Tunnel protocol to associate with the IP phone and to send and receive signaling messages.
- In order to enable Cisco Unified Video Advantage, IP phones have to be video-enabled and regions and locations must be configured to permit video calls.
- Before installing Cisco Unified Video Advantage on the PC, verify hardware and software requirements.
- Cisco Unified Video Advantage includes tools to verify the association with the IP phone, check the camera, and perform diagnostics.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-28

References

For additional information, refer to these resources:

- Installation and Troubleshooting Guide for Cisco Unified Video Advantage Release 2.0
http://www.cisco.com/en/US/docs/video/cuva/2_0/english/adminstration/guide/admin2_0.html
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- Cisco Unified Communications Manager supports software media resources, provided by Cisco Unified Communications Manager servers, as well as external hardware media resources. Media resources include MOH, conference bridges, transcoders, MTPs, and annunciators.
- Cisco Unified Communications Manager supports numerous user features including Call Park, Call Pickup, Hold Reversion, DND, Intercom, Cisco Callback, Barge, and Privacy. IP phone services allow web XML applications to be accessed from Cisco IP phones. Users can reconfigure personal settings such as Call Forward, DND, speed dials, and ring settings by accessing Cisco Unified Communications Manager user web pages.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-1

Module Summary (Cont.)

- Cisco Unified Communications Manager natively supports Presence-enabled speed dials and Presence-enabled call lists and directories.
- Cisco Unified Communications Manager allows seamless and simple integration with voice-mail systems such as Cisco Unity or third-party voice-mail products.
- Cisco Unified Video Advantage extends the capabilities of a Cisco IP phone by adding support for video calls. The video components (camera and display) are provided by a PC attached to the Cisco IP phone while the audio component and call setup function remains at the Cisco IP phone.

© 2008 Cisco Systems, Inc. All rights reserved.

CIPT1 v6.0—5-2

This module describes Cisco Unified Communications Manager support for internal and external media resources and their implementation. The module discusses several user features of Cisco Unified Communications Manager, such as Call Park, Call Pickup, Hold Reversion, DND, Intercom, Cisco Call Back, Barge, and Privacy. It also discusses how XML-based phone services can be accessed from Cisco IP phones and how users can set user-specific phone configuration parameters at the Cisco Unified Communications Manager user web page. Then the module describes the Presence features that are natively supported by Cisco Unified Communications Manager and how these are implemented. Another important part of this module is the discussion on how to integrate Cisco Unified Communications Manager with a voice-mail system. Finally, the module describes how to implement Cisco Unified Video Advantage in order to enable Cisco IP phones and an attached PC to be used for video calls.

References

For additional information, refer to these resources:

- Cisco Unified Communications Manager Features and Services Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmfeat/fsgd.pdf
- Cisco Unified Communications Manager Administration Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf
- Cisco Unified Communications Manager System Guide, Release 6.0(1)
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmsys/accm.pdf
- Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
- Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Release 5.0 – Setting Up a Cisco Unified Communications Manager 6.0 SCCP Integration with Cisco Unity
http://www.cisco.com/en/US/docs/voice_ip_comm/unity/5x/integration/cucm_sccp/guide/cuintcucmskinny080.html
- Installation and Troubleshooting Guide for Cisco Unified Video Advantage Release 2.0
http://www.cisco.com/en/US/docs/video/cuva/2_0/english/adminstration/guide/admin2_0.html

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) Which of these is *not* a supported media resource in Cisco Unified Communications Manager? (Source: Implementing Media Resources)
- A) audio conferencing
 - B) transcoding
 - C) Media Termination Point
 - D) annunciator
 - E) Media Encryption Point
 - F) Music on Hold
- Q2) Which two of the following media resources use one-way audio only? (Choose two.) (Source: Implementing Media Resources)
- A) audio conferencing
 - B) transcoding
 - C) annunciator
 - D) Media Termination Point
 - E) Music on Hold
- Q3) Which two of these statements are true about conference resources? (Choose two.) (Source: Implementing Media Resources)
- A) A software conference bridge can be provided on a Cisco Unified Communications Manager server supporting mixed conferences.
 - B) A hardware conference bridge can support mixed conferences.
 - C) Cisco Unified Communications Manager servers can provide a G.729-only software conference bridge.
 - D) Cisco Unified Communications Manager servers can provide a G.711-only software conference bridge.
 - E) Some phones have a built-in conference bridge supporting G.729.
- Q4) Which configuration step is *not* applicable when implementing hardware conference bridges? (Source: Implementing Media Resources)
- A) Activate the IP Voice Media Streaming Application Service.
 - B) Configure hardware media resources in Cisco Unified Communications Manager.
 - C) Configure hardware media resources in Cisco IOS Software.
 - D) Check if the hardware media resource is registered with Cisco Unified Communications Manager.
- Q5) Which statement is correct about Meet-Me conferences? (Source: Implementing Media Resources)
- A) Meet-Me conferences only work on hardware conference resources.
 - B) Meet-Me conferences only work on software conference resources.
 - C) Meet-Me conferences need to be enabled by configuring a Meet-Me number range (pattern).
 - D) Meet-Me conferences only support G.711.

- Q6) MOH supports which of the following? (Source: Implementing Media Resources)
- A) 51 fixed audio sources
 - B) 51 audio source files
 - C) 50 audio source files and one fixed audio source
 - D) 50 fixed audio sources and 1 audio source file
- Q7) Which two extra steps are required when enabling multicast MOH? (Choose two.) (Source: Implementing Media Resources)
- A) Enable multicast MOH per audio source.
 - B) Enable multicast MOH at each MOH server.
 - C) Enable multicast MOH globally by configuring the appropriate enterprise parameter.
 - D) Enable multicast MOH globally by configuring the appropriate service parameter.
 - E) Enable multicast MOH at the device pools used by the IP phones that should be able to listen to multicast MOH.
- Q8) Which statement is *not* true about the announciator media resource? (Source: Implementing Media Resources)
- A) The announcements support localization and may be customized by replacing the appropriate .wav file.
 - B) The announciator is capable of supporting G.729 and wideband codecs if a transcoder is available.
 - C) The announciator streams spoken messages in order to inform callers about the call progress.
 - D) The announciator is only available as a software media resource.
- Q9) Which of the following load share within their members. (Source: Implementing Media Resources)
- A) media resource group lists
 - B) media resource pools
 - C) media resource groups
 - D) media resource route lists
- Q10) How can media resource group lists be applied to devices? (Source: Implementing Media Resources)
- A) by a device pool or at the line with priority to the device pool
 - B) by a device pool or at the line with priority to the line
 - C) by a device pool or at the device with priority to the device pool
 - D) by a device pool or at the device with priority to the device
- Q11) Which two of the following are *not* user features? (Choose two.) (Source: Configuring Cisco Unified Communications Manager User Features)
- A) auto-registration
 - B) Hold Reversion
 - C) BAT
 - D) Intercom
 - E) Barge and Privacy
 - F) IP Phone Services

- Q12) Which of the following features allows putting a call on hold so that it can be retrieved from another telephone in the cluster? (Source: Configuring Cisco Unified Communications Manager User Features)
- A) Call Hold
 - B) Call Forward
 - C) Call Park
 - D) Dynamic Retrieval
- Q13) What is *not* a valid variant of the Call Pickup feature? (Source: Configuring Cisco Unified Communications Manager User Features)
- A) Call Pickup
 - B) Any Group Pickup
 - C) Other Group Pickup
 - D) Group Pickup
- Q14) Which statement is *not* true about the Intercom feature? (Source: Configuring Cisco Unified Communications Manager User Features)
- A) The Intercom feature uses separate Calling Search Spaces and partitions.
 - B) The Intercom feature starts with a one-way audio stream to the called party.
 - C) Intercom lines can be applied to phone buttons.
 - D) The Intercom feature requires an additional two device license units per Intercom line.
- Q15) Which statement does *not* apply to Barge? (Source: Configuring Cisco Unified Communications Manager User Features)
- A) Barge cannot use conference media resources but is limited to a built-in G.711-only phone conference bridge.
 - B) Barge allows a phone with a shared line to join a call that is active on the shared line at another phone.
 - C) If Privacy is enabled, Barge is not allowed.
 - D) If Privacy is enabled, no call information is shown on other phones that share the line.
- Q16) Which function is *not* provided by the Cisco Unified Communications Manager user web pages? (Source: Understanding Cisco Unified Communications Manager Administration Options)
- A) Forward All Calls
 - B) configure speed dials
 - C) add users
 - D) subscribe to IP phone services
 - E) configure personal address book and speed dials
- Q17) What function is *not* supported by IP phone services? (Source: Configuring Cisco Unified Communications Manager User Features)
- A) displaying data (text and graphics)
 - B) user input
 - C) user authentication
 - D) playing music

- Q18) Which two Presence features are natively supported by Cisco Unified Communications Manager? (Choose two.) (Source: Configuring Presence-Enabled Speed Dials and Lists)
- A) user status information
 - B) Cisco IP phone messenger application
 - C) Presence-enabled speed dials
 - D) third-party Presence server integration
 - E) Presence-enabled directories and call lists
- Q19) Which two endpoints are supported by the Cisco Unified Communications Manager Presence feature? (Choose two.) (Source: Configuring Presence-Enabled Speed Dials and Lists)
- A) Cisco IP phones
 - B) devices that are reached through a SIP trunk
 - C) MGCP gateway endpoints
 - D) H.323 gateways
 - E) voice-mail ports
- Q20) What is *not* a configuration step when enabling Presence? (Source: Configuring Presence-Enabled Speed Dials and Lists)
- A) Customize phone button templates to include Presence-enabled speed dial buttons.
 - B) Enable the BLF for Call Lists enterprise parameter.
 - C) Enable Cisco Unified Communications Manager Presence on SIP trunks.
 - D) Configure the default Presence status in case that the watched phone is unregistered.
- Q21) Which two statements are true about Presence policies? (Choose two.) (Source: Configuring Presence-Enabled Speed Dials and Lists)
- A) Partitions and Subscribe Calling Search Spaces apply to both Presence-enabled speed dials and Presence-enabled lists.
 - B) Presence groups apply to Presence-enabled speed dials.
 - C) Presence groups apply to Presence-enabled lists.
 - D) Interpresence group policies cannot be configured independent in each direction.
 - E) The default intrapresence group policy is to deny subscriptions.
- Q22) Presence groups can be applied to lines, phones (at the device level), and SIP trunks. (Source: Configuring Presence-Enabled Speed Dials and Lists)
- A) true
 - B) false

- Q23) Which three of the following Cisco Unified Communications Manager configuration elements have a direct counterpart in Cisco Unity? (Choose three.) (Source: Integrating Cisco Unified Communications Manager with Voice-Mail Systems)
- A) number of voice-mail ports
 - B) message waiting information
 - C) voice-mail pilot
 - D) voice-mail port name
 - E) line directory number
 - F) hunt list, hunt pilot
 - G) voice-mail profile
- Q24) Which two of the following features are *not* applicable to Cisco Unity? (Choose two.) (Source: Integrating Cisco Unified Communications Manager with Voice-Mail Systems)
- A) ViewMail for Outlook
 - B) multiple languages
 - C) automatic call distribution (call center function)
 - D) text-to-speech
 - E) third-party fax
 - F) voice recognition for outgoing e-mails
- Q25) The voice-mail pilot is used when calls are forwarded to voice mail by specifying the hunt pilot number as the call forward destination. (Source: Integrating Cisco Unified Communications Manager with Voice-Mail Systems)
- A) true
 - B) false
- Q26) What are two possible reasons that calls forwarded to voice mail do not reach the voice-mail system? (Choose two.) (Source: Integrating Cisco Unified Communications Manager with Voice-Mail Systems)
- A) The Call Forward to Voice Mail check box has been activated but the calling search space of the voice-mail profile does not have access to the partition of the hunt pilot.
 - B) The Call Forward to Voice Mail check box has been activated but the calling search space of the forwarding line does not have access to the partition of the hunt pilot.
 - C) The hunt pilot number has been specified as a call forward destination but the call forward calling search space at the line does not have access to the partition of the hunt pilot.
 - D) The hunt pilot number has been specified as a call forward destination but the call forward calling search space does not have access to the partition of the hunt list.
 - E) The Call Forward to Voice Mail check box has been activated but the calling search space of the voice mail profile does not have access to the partition of the voice-mail port.
- Q27) Which of the following is *not* part of the Cisco Unity integration configuration steps? (Source: Integrating Cisco Unified Communications Manager with Voice-Mail Systems)
- A) Configuring IP addresses of Cisco Unified Communications Manager servers
 - B) Configuring MWI numbers
 - C) Configuring voice-mail port name (prefix) and number of voice-mail ports
 - D) Configuring the number of the hunt pilot

- Q28) The name of the Cisco Unity subscriber must match the end user name in Cisco Unified Communications Manager in order to be able to retrieve voice mails from the phone. (Source: Integrating Cisco Unified Communications Manager with Voice-Mail Systems)
- A) true
B) false
- Q29) Which two of the following statements are *not* required for Cisco Unified Video Advantage to work? (Choose two.) (Source: Implementing Cisco Unified Video Advantage)
- A) A video conference bridge must be present.
B) A PC must be equipped with a Cisco Unified VT Camera and needs the Cisco Unified Video Advantage software installed.
C) The PC must be physically connected to a Cisco IP phone or Cisco IP Communicator must be used on the PC.
D) The enterprise parameter that enables video must be configured.
E) Phones must be configured to use the G.711 codec.
- Q30) Which two of the following protocols are used by Cisco Unified Video Advantage? (Choose two.) (Source: Implementing Cisco Unified Video Advantage)
- A) Cisco Audio Session Tunnel
B) FTP
C) IPsec
D) Cisco Discovery Protocol
E) SSH
- Q31) Cisco IP phones must be enabled to support video. (Source: Implementing Cisco Unified Video Advantage)
- A) true
B) false
- Q32) Which of the following is *not* a hardware requirement for Cisco Unified Video Advantage? (Source: Implementing Cisco Unified Video Advantage)
- A) at least 1.9 GHz CPU
B) at least 2048 MB memory
C) at least one USB port
D) connected to a Cisco Unified IP phone or colocated with Cisco IP Communicator
E) Cisco VT Camera connected to a USB port of the PC
- Q33) Which of the following is *not* a verification tool provided by Cisco Unified Video Advantage? (Source: Implementing Cisco Unified Video Advantage)
- A) connection status
B) video check
C) diagnostics
D) packet sniffer

Module Self-Check Answer Key

- Q1) E
- Q2) C, E
- Q3) B, D
- Q4) A
- Q5) C
- Q6) C
- Q7) A, B
- Q8) B
- Q9) C
- Q10) D
- Q11) A, C
- Q12) C
- Q13) B
- Q14) D
- Q15) A
- Q16) C
- Q17) D
- Q18) C, E
- Q19) A, B
- Q20) D
- Q21) A, C
- Q22) A
- Q23) C, F, G
- Q24) C, F
- Q25) B
- Q26) A, C
- Q27) D
- Q28) B
- Q29) B, C
- Q30) A, D
- Q31) A
- Q32) B
- Q33) D