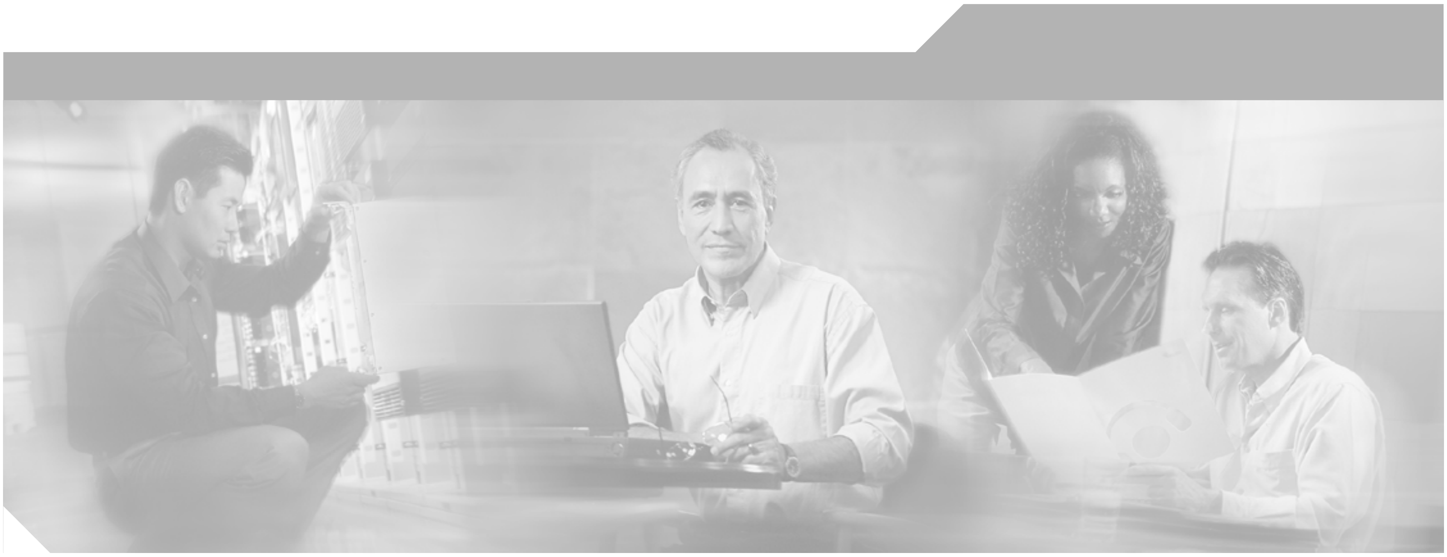


Cisco CallManager Features and Services Guide

Release 5.0(1)

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8141-01

Cisco CallManager Features and Services Guide

CONTENTS

Preface xxi

Purpose xxi

Audience xxi

Organization xxii

Related Documentation xxiii

Conventions xxiii

Obtaining Documentation xxiv

Cisco.com xxv

Product Documentation DVD xxv

Ordering Documentation xxv

Documentation Feedback xxv

Cisco Product Security Overview xxvi

Reporting Security Problems in Cisco Products xxvi

Obtaining Technical Assistance xxvii

Cisco Technical Support & Documentation Website xxvii

Submitting a Service Request xxviii

Definitions of Service Request Severity xxviii

Obtaining Additional Publications and Information xxviii

CHAPTER 1 Cisco CallManager Extension Mobility 1-1

Introducing Cisco CallManager Extension Mobility 1-1

Understanding Device Profiles 1-2

User Device Profile 1-2

Autogenerated Device Profile 1-2

Default Device Profile 1-2

Overview of Cisco CallManager Extension Mobility 1-3

SIP Support for Extension Mobility 1-5

Login and Logout Behavior 1-5

Login Call Flow 1-6

Logout Call Flow 1-7

System Requirements for Cisco CallManager Extension Mobility 1-7

Interactions and Restrictions 1-8

Interactions 1-8

Cisco CallManager Services That are Running on the Same Server 1-8

Bulk Administration Tool 1-9

Cisco IP Manager Assistant 1-9

Cisco CallManager Attendant Console 1-9

Call Display Restrictions 1-9

Restrictions 1-10

Installing Cisco CallManager Extension Mobility for the First Time 1-10

Configuring Cisco CallManager Extension Mobility 1-11

Configuration Guidelines 1-11

Configuration Example 1 1-12

Configuration Example 2 1-12

Configuration Checklist for Cisco CallManager Extension Mobility 1-13

Adding the Cisco CallManager Extension Mobility Service 1-15

Setting the Service Parameters 1-16

Creating a Device Profile Default for Each Cisco IP Phone Model 1-18

Creating the Device Profile for a User 1-20

Associating a User Device Profile to a User 1-23

Subscribing Cisco IP Phones to Cisco CallManager Extension Mobility 1-24

Providing Information to Cisco CallManager Extension Mobility Users 1-26

Related Topics 1-26

CHAPTER 2 **Cisco IP Manager Assistant With Proxy Line Support** 2-1

Introducing Cisco IPMA 2-1

Cisco IPMA Architecture Overview 2-2

Cisco IPMA Service 2-2

Assistant Console Interface 2-4

Cisco IP Phone Interface 2-4

Cisco IPMA Database Access Architecture 2-5

Manager Interfaces 2-5

Assistant Interfaces 2-5

Softkeys 2-5

Manager Assistant Administration Interface 2-6

System Requirements for Cisco IPMA with Proxy Line Support 2-6

Interactions and Restrictions 2-7

Interactions 2-7

Bulk Administration Tool 2-7

Extension Mobility 2-7

Reporting Tools 2-8

Multilevel Precedence and Preemption (MLPP) 2-9

Time-of-Day Routing 2-9

Restrictions 2-9

Installing and Activating Cisco IPMA 2-10

Configuring Cisco IPMA with Proxy Line Support 2-10

Configuration Checklist for Cisco IPMA with Proxy Line Support 2-11

System Configuration with Proxy Line Support 2-13

Cisco IPMA Configuration Wizard 2-13

Calling Search Space and Partitions 2-16

Cisco IPMA Route Point 2-17

Setting the Service Parameters for Cisco IPMA 2-18

Security Considerations 2-20

Starting the Cisco IPMA Service 2-20

Cisco IP Phone Service Configuration 2-20

Manager and Assistant Phone Configuration 2-21

Manager Phones 2-22

Assistant Phones 2-23

Nonmanager and Nonassistant Phones 2-24

Manager and Assistant Configuration 2-24

Configuring a Manager and Assigning an Assistant for Proxy Line Mode 2-25

Deleting Cisco IPMA Information from the Manager 2-26

Updating the Manager Cisco IPMA Configuration 2-27

Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant 2-28

Deleting the Cisco IPMA Information from the Assistant 2-29

Updating the Assistant Cisco IPMA Configuration 2-30

Dial Rules Configuration 2-31

Providing Information to Cisco IPMA Managers and Assistants 2-31

Installing the Assistant Console Application 2-32

Assistant Console Dialog Options 2-32

Manager Configuration 2-32

Related Topics 2-33

CHAPTER 3 **Cisco IP Manager Assistant With Shared Line Support** 3-1

Introducing Cisco IPMA 3-1

Cisco IPMA Architecture Overview 3-2

Cisco IPMA Service 3-2

Assistant Console Interface 3-3

Cisco IP Phone Interface 3-4

Cisco IPMA Database Access Architecture 3-4

Manager Interfaces 3-4

Assistant Interfaces 3-4

Softkeys 3-4

Manager Assistant Administration Interface 3-5

System Requirements for Cisco IPMA with Shared Line Support 3-5

Interactions and Restrictions 3-6

Interactions 3-6

Bulk Administration Tool 3-6

Extension Mobility 3-6

Reporting Tools 3-7

Multilevel Precedence and Preemption (MLPP) 3-8

Restrictions 3-8

Installing and Activating Cisco IPMA 3-8

Configuring Cisco IPMA with Shared Line Support 3-9

Configuration Checklist for Cisco IPMA with Shared Line Support 3-9

Setting the Service Parameters for Cisco IPMA 3-11

Security Considerations 3-13

Starting the Cisco IPMA Service 3-13

Manager and Assistant Phone Configuration 3-13

Manager Phones 3-14

Assistant Phones 3-14

Nonmanager and Nonassistant Phones 3-15

Manager and Assistant Configuration 3-15

Configuring a Manager and Assigning an Assistant for Shared Line Mode 3-16

Deleting Cisco IPMA Information for the Manager 3-17

Updating the Manager Cisco IPMA Configuration 3-18

Configuring Shared and Incoming Intercom Lines for the Assistant 3-18

Deleting the Cisco IPMA Information for the Assistant 3-20

Updating the Assistant Cisco IPMA Configuration 3-20

Dial Rules Configuration 3-21

Providing Information to Cisco IPMA Managers and Assistants 3-22

Installing the Assistant Console Application 3-22

Assistant Console Dialog Options 3-22

Manager Configuration 3-23

Related Topics 3-23

CHAPTER 4 Cisco Call Back 4-1

Introducing Cisco Call Back 4-1

Understanding How Cisco Call Back Works 4-2

Suspend/Resume Functionality for Call Back 4-4

System Requirements for Cisco Call Back 4-4

Interactions and Restrictions 4-5

Additional Information on Cisco Call Back Notification with SIP Phones 4-5

Feature Interactions with Call Forward, iDivert, and Voice-Messaging System Features 4-6

Installing and Configuring Cisco Call Back 4-6

Configuration Checklist for Cisco Call Back 4-7

Creating a Softkey Template for the CallBack Softkey 4-7

Configuring CallBack Softkey Template in Device Pool 4-8

Adding CallBack Softkey Template in Phone Configuration 4-9

Setting Cisco Call Back Service Parameters 4-9

Providing Cisco Call Back Information to Users 4-10

Troubleshooting Cisco Call Back 4-10

Related Topics 4-10

CHAPTER 5 Client Matter Codes and Forced Authorization Codes 5-1

Introducing Client Matter Codes 5-2

Introducing Forced Authorization Codes 5-2

Interactions and Restrictions 5-3

Using the Cisco Bulk Administration Tool (BAT) 5-4

Using CDR Analysis and Reporting (CAR) 5-4

Using FAC/CMC with CTI, JTAPI, and TAPI Applications 5-4

System Requirements 5-5

Installation of CMC and FAC 5-5

CMC and FAC Configuration Checklist 5-5

Client Matter Codes Configuration 5-6

Finding Client Matter Codes 5-6

Configuring Client Matter Codes 5-7

Deleting Client Matter Codes 5-8

CMC Configuration Settings 5-8

Enabling Client Matter Codes For Route Patterns 5-8

Forced Authorization Codes Configuration 5-9

Finding Forced Authorization Codes 5-9

Configuring Forced Authorization Codes 5-10

Deleting Forced Authorization Codes 5-11

FAC Configuration Settings 5-11

Enabling Forced Authorization Codes for Route Patterns 5-12

Providing Information to Users 5-13

Related Topics 5-13

CHAPTER 6 Music On Hold 6-1

Understanding Music On Hold 6-1

Music On Hold Definitions 6-2

Music On Hold Characteristics 6-3

Music On Hold Functionality 6-4

User Hold Example 6-5

Transfer Hold Example 6-5

Call Park Example 6-5

Supported Music On Hold Features 6-5

Music On Hold Server 6-8

Music On Hold Audio Sources 6-8

Default Music On Hold Sample 6-9

Creating Audio Sources 6-9

Storing Audio Source Files 6-9

Managing Audio Sources 6-10

Multicast and Unicast Audio Sources 6-10

Multicast Configuration Checklist 6-11

Music On Hold System Requirements and Limits 6-12

Music On Hold Failover and Fallback 6-13

Music On Hold Configuration Checklist 6-14

Monitoring Music On Hold Performance 6-15

Viewing Music On Hold Server Performance 6-15

Checking Service States 6-16

Music On Hold Audio Source Configuration 6-16

Finding a Music On Hold Audio Source 6-17

Configuring a Music On Hold Audio Source 6-18

Deleting a Music On Hold Audio Source 6-19

Music On Hold Audio Source Configuration Settings 6-19

Fixed Music On Hold Audio Source Configuration 6-21

Configuring the Fixed Music On Hold (MOH) Audio Source 6-22

Deleting a Fixed Music On Hold (MOH) Audio Source 6-22

Fixed Music On Hold (MOH) Audio Source Configuration Settings 6-23

Music On Hold Server Configuration 6-23

Finding a Music On Hold Server 6-23

Configuring a Music On Hold Server 6-24

Resetting or Restarting a Music On Hold Server 6-25
Music On Hold Server Configuration Settings 6-26
Related Topics 6-28

CHAPTER 7 Cisco CallManager AutoAttendant 7-1
Understanding Cisco CallManager AutoAttendant 7-1
Cisco CallManager AutoAttendant Overview 7-2
Components of Cisco CallManager AutoAttendant 7-3
Installing and Upgrading the Customer Response Solutions (CRS) Engine 7-3
Hardware and Software Requirements 7-3
Installing or Upgrading Cisco CallManager AutoAttendant 7-4
Installing Cisco CallManager AutoAttendant 7-4
Configuring Cisco CallManager AutoAttendant and the CRS Engine 7-4
Configuration Checklist for Cisco CallManager AutoAttendant 7-5
Configuring Cisco CallManager 7-5
Configuring a Cisco CallManager User for Cisco CallManager AutoAttendant 7-5
Configuring the Cisco Customer Response Solutions Engine 7-9
Cluster Setup 7-10
Server Setup 7-11
Adding a JTAPI Call Control Group 7-11
Provisioning Cisco Media Termination Subsystem 7-15
Adding a New Cisco CallManager AutoAttendant 7-16
Configuring a JTAPI Trigger 7-17
Customizing Cisco CallManager AutoAttendant 7-20
Modifying an Instance of Cisco CallManager AutoAttendant 7-20
Configuring Prompts 7-21
Managing Cisco CallManager AutoAttendant 7-24
Related Topics 7-24

CHAPTER 8 Barge and Privacy 8-1
Introducing Barge and Privacy 8-1
Barge 8-1
Barge Using Built-In Conference—Barge Softkey 8-3
Barge Using Shared Conference—cBarge Softkey 8-4
Privacy 8-4
System Requirements for Barge and Privacy 8-5

Interactions and Restrictions 8-6
Interactions 8-6
Barge and cBarge 8-6
Barge and Call Park 8-6
Barge and Join 8-6
Restrictions 8-6
Installing and Activating Barge and Privacy 8-8
Activating Barge with Built-In Conference Bridge 8-8
Activating cBarge with Shared Conference Bridge 8-8
Activating Privacy 8-8
Configuring Barge and Privacy 8-8
Barge Configuration Checklist 8-9
Privacy Configuration Checklist 8-10
Setting the Service Parameters for Barge and Privacy 8-10
Related Topics 8-11
CHAPTER 9 Call Park 9-1
Introducing Call Park 9-1
System Requirements for Call Park 9-4
Interactions and Restrictions 9-4
Interactions 9-4
CTI Applications 9-4
Music On Hold 9-5
Route Plan Report 9-5
Calling Search Space and Partitions 9-5
Immediate Divert 9-5
Barge 9-5
Restrictions 9-6
Installing and Activating Call Park 9-6
Configuring Call Park 9-6
Call Park Configuration Checklist 9-6
Setting the Service Parameters for Call Park 9-7
Finding a Call Park Number 9-7
Configuring a Call Park Number 9-9
Call Park Configuration Settings 9-10
Deleting a Call Park Number 9-11
Troubleshooting Call Park 9-11
Related Topics 9-12

CHAPTER 10 **Call Pickup Group** 10-1

Introducing Call Pickup Group 10-1

Auto Call Pickup 10-2

Call Pickup No Answer 10-3

Call Pickup Busy 10-3

Call Pickup No Bandwidth 10-3

Using Call Pickup Features with Partitions to Restrict Access 10-3

System Requirements for Call Pickup Group 10-3

Interactions and Restrictions 10-4

Interactions 10-4

Route Plan Report 10-4

Calling Search Space and Partitions 10-4

Time of Day 10-4

Call Accounting 10-5

Dependency Records 10-5

Restrictions 10-5

Installing and Activating Call Pickup Group 10-6

Configuring Call Pickup Group 10-6

Call Pickup Group Configuration Checklist 10-6

Other Group Call Pickup Configuration Checklist 10-8

Setting the Service Parameters for Call Pickup Group 10-9

Finding a Call Pickup Group 10-10

Configuring a Call Pickup Group 10-11

Call Pickup Group Configuration Settings 10-12

Deleting a Call Pickup Group 10-13

Defining a Pickup Group for Other Group Call Pickup 10-13

Assigning A Call Pickup Group to Directory Numbers 10-14

Related Topics 10-15

CHAPTER 11 **Immediate Divert** 11-1

Introducing Immediate Divert 11-1

System Requirements for Immediate Divert 11-2

Call-Processing Requirements for Immediate Divert 11-2

Softkey Requirements 11-2

Incoming Calls Requirements 11-2

Outgoing Calls Requirements 11-3

Immediate Divert Phone Display Messages 11-3

Using Immediate Divert 11-4

Interactions and Restrictions 11-5
Interactions 11-5
Multilevel Precedence and Preemption (MLPP) 11-5
Call Forward 11-5
Call Detail Records (CDR) 11-6
Conference 11-6
Hunt List 11-6
Restrictions 11-6
Installing and Activating Immediate Divert 11-7
Configuring Immediate Divert 11-7
Immediate Divert Configuration Checklist 11-7
Setting the Service Parameter for Immediate Divert 11-8
Where to Find More Information 11-8
Related Topics 11-8
CHAPTER 12 Malicious Call Identification 12-1
Introducing Malicious Call Identification 12-1
Using the Malicious Call ID Feature with Cisco CallManager 12-2
System Requirements for Malicious Call ID 12-2
Interactions and Restrictions 12-2
Interactions 12-2
Conference Calls 12-3
Extension Mobility 12-3
Call Detail Records 12-3
Alarms 12-3
Restrictions 12-4
Installing Malicious Call ID 12-4
Configuring Malicious Call ID 12-4
Malicious Call ID Configuration Checklist 12-4
Setting the Service Parameter for Malicious Call ID 12-5
Configuring Alarms for Malicious Call ID 12-6
Adding a Softkey Template for Malicious Call ID 12-6
Giving the Malicious Call Identification Feature to Users 12-7
Removing the Malicious Call Identification Feature from a User 12-7
Troubleshooting Malicious Call ID 12-8
Related Topics 12-8

CHAPTER 13 Multilevel Precedence and Preemption 13-1

Introducing MLPP 13-1

MLPP Terminology 13-2

Precedence 13-3

Executive Override Precedence Level 13-3

Executive Override Precedence Call Setup 13-4

Executive Override Precedence Calls Across the PRI 4ESS Interface 13-5

PRI 4ES UUIE-Based MLPP Interface to DRSN 13-5

Preemption 13-6

Domain 13-6

Location-Based MLPP 13-6

MLPP Over Intercluster Trunks 13-7

MLPP Precedence Patterns 13-7

MLPP Indication Enabled 13-7

Precedence Call Setup 13-8

Alternate Party Diversion 13-9

MLPP Preemption Enabled 13-10

Receiving Preemption 13-10

Preemption Enabled 13-10

Preemption Details 13-11

User Access Preemption 13-11

User Access Channel Nonpreemptable 13-12

Common Network Facility Preemption 13-12

Location-Based Preemption 13-14

MLPP Announcements 13-16

Unauthorized Precedence Announcement 13-17

Blocked Precedence Announcement 13-18

Busy Station Not Equipped for Preemption 13-18

Announcements Over Intercluster Trunks 13-18

MLPP Numbering Plan Access Control for Precedence Patterns 13-19

MLPP Trunk Selection 13-21

MLPP Hierarchical Configuration 13-23

Service Parameter Special Trace Configuration 13-23

CDR Recording for Precedence Calls 13-24

Line Feature Interaction 13-24

Call Forward 13-24

Call Transfer 13-25

Shared Lines 13-25

Call Waiting 13-25

Call Preservation 13-26
Automated Alternate Routing 13-26
MGCP and PRI Protocol 13-26
Secure Endpoints and Secure Communications 13-26
Interactions and Restrictions 13-26
Interactions 13-27
Restrictions 13-27
Installing and Activating MLPP 13-28
MLPP Configuration Checklist 13-28
Setting the Enterprise Parameters for MLPP 13-29
Related Topics 13-30

CHAPTER 14 **Custom Phone Rings** 14-1
Introducing Custom Phone Rings 14-1
Customizing and Modifying Configuration Files 14-2
Ringlist.xml File Format Requirements 14-2
PCM File Requirements for Custom Ring Types 14-3
Configuring a Custom Phone Ring 14-3
Related Topics 14-3

CHAPTER 15 **Cisco WebDialer** 15-1
Introducing Cisco WebDialer 15-1
Webdialer Servlet 15-1
Redirector Servlet 15-2
Redundancy 15-2
System Requirements for Cisco WebDialer 15-3
Interactions and Restrictions 15-3
Interactions 15-3
Restrictions 15-4
Installing and Activating Cisco WebDialer 15-4
Configuring Cisco WebDialer 15-5
Cisco WebDialer Configuration Checklist 15-5
Configuring the Webdialer Servlet 15-6
Setting Service Parameters for the Webdialer Servlet 15-6
Configuring the Application User 15-7
Secure TLS Connection to CTI 15-7
Configuring WebDialer for the Local Language 15-8

Partition Support 15-9

Configuring the Redirector Servlet (Optional) 15-9

Configuring Application Dial Rules (Optional) 15-10

Adding Users to the Standard Cisco CallManager End Users Group 15-10

Creating a Proxy User (Optional) 15-11

Trace Settings (optional) 15-12

Related Topics 15-13

CHAPTER 16 **Cisco CallManager Attendant Console** 16-1

Introducing Cisco CallManager Attendant Console 16-1

Understanding Cisco CallManager Attendant Console Users 16-2

Understanding Pilot Points and Hunt Groups 16-2

Understanding Linked Hunt Groups 16-5

Understanding Circular Hunt Groups 16-6

Understanding Broadcast Hunting 16-8

Understanding Call Queuing 16-9

Understanding the Cisco CallManager Attendant Console Directory 16-9

Understanding the Cisco CallManager Attendant Console Server 16-10

Cisco CallManager Attendant Console Redundancy 16-11

System Requirements for Cisco CallManager Attendant Console 16-12

Attendant PC Requirements 16-12

Cisco IP Phone and Voice-Messaging Requirements for Use with the Attendant Console 16-12

Interactions and Restrictions 16-13

Interactions 16-13

Cisco CallManager Extension Mobility 16-13

Music On Hold 16-13

Call Park 16-13

CTI 16-14

Restrictions 16-14

Installing and Activating Cisco CallManager Attendant Console 16-15

Configuring Cisco CallManager Attendant Console 16-15

Configuration Checklist for Cisco CallManager Attendant Console 16-16

Configuring Cisco CallManager Attendant Console Users 16-17

Finding an Attendant Console User 16-17

Configuring an Attendant Console User 16-19

Cisco CallManager Attendant Console User Configuration Settings 16-19

Deleting an Attendant Console User 16-20

Configuring the ac User 16-20

Configuring Pilot Points 16-21
Finding a Pilot Point 16-22
Configuring a Pilot Point 16-23
Pilot Point Configuration Settings 16-24
Deleting a Pilot Point 16-26
Resetting a Pilot Point 16-26
Associating Devices and Pilot Points with the ac User 16-27
Configuring Hunt Groups 16-28
Configuring Hunt Group Members 16-28
Hunt Group Configuration Settings 16-29
Deleting Hunt Group Members 16-30
Cisco CallManager Attendant Console Server Configuration 16-31
Creating and Uploading the CorporateDirectory.txt File 16-31
Deleting the CorporateDirectory.txt File 16-33
Installing the Cisco CallManager Attendant Console Plug-in on an Attendant PC 16-33
Starting Cisco CallManager Attendant Console After Installing Windows XP SP2 16-34
Configuring Cisco CallManager Attendant Console Settings 16-35
Attendant Console Configuration Settings 16-35
Configuring Held Icon Timers 16-37
Dependency Records 16-38
Troubleshooting Cisco CallManager Attendant Console 16-38
Related Topics 16-39
CHAPTER 17 Call Display Restrictions 17-1
Introducing Call Display Restrictions 17-1
Overview of Call Display Restrictions 17-2
Enabling Call Display Restrictions 17-2
System Requirements for Call Display Restrictions 17-3
Scenarios for Using Call Display Restrictions 17-3
Interactions 17-3
Call Park 17-4
Conference List 17-4
Conference and Voice Mail 17-4
Extension Mobility 17-4
Configuring Call Display Restrictions 17-5
Call Display Restrictions Configuration Checklist 17-5
Configuring the Translation Pattern Parameters 17-6
Configuring the Phone Configuration 17-7

Sample Configurations 17-8

Partitions 17-8

Calling Search Spaces 17-8

Devices and Gateways 17-9

Translation Patterns 17-9

Call Park 17-11

Sample Call Flow 17-12

Related Topics 17-12

CHAPTER 18 **Quality Report Tool** 18-1

Introducing Quality Report Tool 18-1

Components of QRT 18-2

Overview of QRT Architecture 18-3

Cisco CTIManager Interface (QBEHelper) 18-4

Cisco CallManager Database Interface (DBL Library) 18-4

Screen Helper and Dictionary 18-4

Redundancy Manager 18-4

DB Change Notifier 18-5

SDI Trace and Alarm 18-5

System Requirements for QRT 18-5

Cisco Extended Functions Service Dependency 18-5

Multiple Cisco Extended Functions Applications in a Cluster 18-6

Securing a TLS Connection to CTI 18-7

How to Use QRT 18-8

User Interface 18-8

Extended Menu Choices 18-9

Problem Classification Categories and Reason Codes 18-10

Interactions and Restrictions 18-14

Installing and Activating QRT Functions 18-14

Configuring the QRT Feature 18-15

Configuration Checklist for QRT 18-16

Creating a Softkey Template with the QRT Softkey 18-16

Configuring the QRT Softkey Template in Device Pool 18-19

Adding the QRT Softkey Template in Phone Configuration 18-20

Configuring the Cisco CallManager Serviceability Features 18-21

Activating the Cisco Extended Functions Service for QRT 18-22

Configuring Alarms and Traces for QRT 18-23

Setting the Cisco Extended Functions Service Parameters for QRT 18-24

Using the QRT Viewer 18-26
QRT Reports 18-26
Providing Information to Users for the QRT Feature 18-31
Troubleshooting the QRT Feature 18-31
Related Topics 18-32

CHAPTER 19 External Call Transfer Restrictions 19-1
Introducing External Call Transfer Restrictions 19-1
System Requirements for External Call Transfer Restrictions 19-4
Interactions and Restrictions 19-4
Interactions 19-5
Restrictions 19-5
Installing and Activating External Call Transfer Restrictions 19-5
Configuring External Call Transfer Restrictions 19-6
External Call Transfer Restrictions Configuration Checklist 19-6
Configuring External Call Transfer Restrictions Service Parameters 19-7
Configuring Transfer Capabilities by Using Call Classification Service Parameter 19-7
Setting the Block OffNet to OffNet Transfer Service Parameter 19-7
Configuring Transfer Capabilities by Using Gateway Configuration 19-7
Configuring Transfer Capabilities by Using Trunk Configuration 19-8
Configuring Transfer Capabilities by Using Route Pattern Configuration 19-8
Related Topics 19-9

CHAPTER 20 Presence 20-1
Introducing Presence 20-2
Understanding How Presence Works with Phones and Trunks 20-2
Understanding How Presence Works with Route Lists 20-4
Understanding Presence Groups 20-4
Understanding Presence Authorization 20-7
Understanding How the SUBSCRIBE Calling Search Space Works 20-8
Understanding How Presence Works with Extension Mobility 20-9
Presence Feature Interactions/Restrictions 20-9
Presence Configuration Checklist 20-10
Configuring Presence Service Parameters and Enterprise Parameters 20-12
Configuring and Applying the SUBSCRIBE Calling Search Space 20-13
Finding Presence Groups 20-14
Configuring Presence Groups 20-15

Presence Group Configuration Settings 20-15

Deleting a Presence Group 20-16

Applying a Presence Group 20-17

Presence Group and Presence Authorization Tips 20-18

Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons 20-18

Configuring BLF/SpeedDial Buttons 20-19

BLF/SpeedDial Configuration Settings 20-20

Where to Find More Information 20-21

INDEX

Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

Note This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at this URL:

http://www.cisco.com/univercd/home/home.htm

The preface covers these topics:

- Purpose, page xxi
- Audience, page xxi
- Organization, page xxii
- Related Documentation, page xxiii
- Conventions, page xxiii
- Obtaining Documentation, page xxiv
- Documentation Feedback, page xxv
- Cisco Product Security Overview, page xxvi
- Obtaining Technical Assistance, page xxvii
- Obtaining Additional Publications and Information, page xxviii

Purpose

The *Cisco CallManager Features and Services Guide* provides the information that you need to understand, install, configure, manage, use, and troubleshoot Cisco CallManager features.

Audience

The *Cisco CallManager Features and Services Guide* provides information for network administrators who are responsible for managing the Cisco CallManager system. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table provides an overview of the organization of this guide.

Chapter	Description
Cisco CallManager Extension Mobility	Provides a description and configuration procedures for Cisco CallManager Extension Mobility for Cisco CallManager.
Cisco IP Manager Assistant With Proxy Line Support	Provides a description and configuration procedures for Cisco IP Manager Assistant (Cisco IPMA) with proxy line support.
Cisco IP Manager Assistant With Shared Line Support	Provides a description and configuration procedures for Cisco IP Manager Assistant (Cisco IPMA) with shared line support.
Cisco Call Back	Provides a description and configuration procedures for Cisco Call Back.
Client Matter Codes and Forced Authorization Codes	Provides descriptions and configuration procedures for Client Matters Codes (CMC) and Forced Authorization Codes (FAC).
Music On Hold	Provides a description and configuration procedures for Cisco Music On Hold.
Cisco CallManager AutoAttendant	Provides a description and configuration procedures for Cisco CallManager AutoAttendant.
Barge and Privacy	Provides a description and configuration procedures for the Cisco CallManager features Barge and Privacy.
Call Park	Provides a description and configuration procedures for the Cisco CallManager Call Park feature.
Call Pickup Group	Provides a description and configuration procedures for the Call Pickup feature.
Immediate Divert	Provides a description and configuration procedures for the Cisco CallManager Immediate Divert feature.
Malicious Call Identification	Provides a description and configuration procedures for the Cisco CallManager Malicious Call Identification feature.
Multilevel Precedence and Preemption	Provides a description and configuration procedures for the Cisco CallManager Multilevel Precedence and Preemption feature.
Custom Phone Rings	Provides a description and configuration procedures for Cisco CallManager custom phone rings.
Cisco WebDialer	Provides a description and configuration procedures for Cisco WebDialer for Cisco CallManager.
Cisco CallManager Attendant Console	Provides a description and configuration procedures for the Cisco CallManager Attendant Console application.
Call Display Restrictions	Provides a description and configuration procedures for the Call Display Restrictions feature.
Quality Report Tool	Provides a description and configuration procedures for the Quality Report Tool (QRT) feature.

Chapter	Description
External Call Transfer Restrictions	Provides a description and configuration procedures for the External Call Transfer Restrictions feature.
Presence	Provides a description and configuration procedures for the Presence feature.

Related Documentation

Refer to the following documents for further information about related Cisco IP telephony applications and products:

- *Installing Cisco CallManager Release 5.0(1)*
- *Upgrading Cisco CallManager Release 5.0(1)*
- *Release Notes for Cisco CallManager Release 5.0(1)*
- *Cisco CallManager System Guide*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Troubleshooting Guide for Cisco CallManager*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- *Cisco CallManager Bulk Administration Guide*
- *Cisco CallManager Security Guide*

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.

Convention	Description
⟶	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.
Action>Reports	Command paths in a graphical user interface (GUI).

Notes use the following convention:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following convention:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Cisco CallManager Extension Mobility

The Cisco CallManager Extension Mobility feature allows users to temporarily access their Cisco IP Phone configuration such as line appearances, services, and speed dials from other Cisco IP Phones.

With Cisco CallManager 4.0 or later, extension mobility functionality extends to most Cisco IP Phone models. You can configure each Cisco IP Phone model to support Cisco CallManager Extension Mobility by using the Device Profile Default window in Cisco CallManager Administration. This allows users who do not have a user device profile for a particular Cisco IP Phone model to use Cisco CallManager Extension Mobility with that phone model.

Note Check the Cisco IP Phone model documentation to verify that Cisco CallManager Extension Mobility is supported.

This chapter provides the following information about Cisco CallManager Extension Mobility:

- Introducing Cisco CallManager Extension Mobility, page 1-1
- System Requirements for Cisco CallManager Extension Mobility, page 1-7
- Interactions and Restrictions, page 1-8
- Installing Cisco CallManager Extension Mobility for the First Time, page 1-10
- Configuring Cisco CallManager Extension Mobility, page 1-11
- Providing Information to Cisco CallManager Extension Mobility Users, page 1-26
- Related Topics, page 1-26

Introducing Cisco CallManager Extension Mobility

The following sections will help you to understand Cisco CallManager Extension Mobility, so you can configure and troubleshoot the feature:

- Understanding Device Profiles, page 1-2
- Overview of Cisco CallManager Extension Mobility, page 1-3
- Login and Logout Behavior, page 1-5
- Login Call Flow, page 1-6
- Logout Call Flow, page 1-7

Understanding Device Profiles

A device profile defines the attributes of a particular device. A device profile includes information such as the phone template, user locale, subscribed services, and speed dials.

The device profile does not get associated with a physical phone. It includes all the properties of a device except those that are explicitly tied to a device, such as MAC address or directory URL.

When a device profile has been loaded onto a device, the device adopts the attributes of that device profile.

User Device Profile

As system administrator, you configure a user device profile for each individual user. Using the Cisco CallManager User Options window, a user can access this profile and make changes, such as adding a service. You can add, modify or delete a user device profile in Cisco CallManager Administration.

When a user logs in to a phone that is configured for Cisco CallManager Extension Mobility and the user has a user device profile that is configured for that phone, the user device profile replaces the existing configuration of the device.

When a user logs out, the logout profile replaces the user device profile.

Autogenerated Device Profile

The autogenerated device profile represents a special device profile that gets generated when you configure a phone for Cisco CallManager Extension Mobility and choose “Use Current Settings” from the Phone Configuration window. The autogenerated device profile then associates with a specific phone to be the logout device profile.

Note Cisco strongly recommends that you configure Cisco CallManager Extension Mobility to use the autogenerated device profile as the logout profile, not the user device profile.

You cannot associate an autogenerated device profile with a user. An autogenerated device profile can be loaded onto a device only when no user is logged in.

When you make changes to a phone and update it, the update may overwrite modifications of the autogenerated device profile.

Default Device Profile

With Cisco CallManager 4.0 or later, you can configure a default device profile for each Cisco IP Phone model that you want to support Cisco CallManager Extension Mobility. The phone takes on the default device profile whenever a user logs in to a phone model for which that user does not have a user device profile.

A default device profile includes device type (phone model), user locale, phone button template, softkey template, and multilevel precedence and preemption (MLPP) information.

You create a default device profile by using the Default Device Profile Configuration window. A phone model can have zero or one device profile default. The maximum number of default device profiles cannot exceed the number of phone models that support Cisco CallManager Extension Mobility.

Overview of Cisco CallManager Extension Mobility

Cisco CallManager Extension Mobility (an XML-based authentication feature) comprises the Cisco Extension Mobility application service and the Cisco Extension Mobility service. The following feature services need to be activated from the Cisco CallManager Serviceability pages for EM to be enabled:

- Cisco Extension Mobility
- Cisco CallManager Cisco IP Phone Services

The Cisco Extension Mobility service runs as an application on the Cisco Tomcat Web Service. Cisco CallManager Extension Mobility works on phones within a single Cisco CallManager cluster only.

You can activate/deactivate these services from **Cisco CallManager Serviceability > Service Activation**. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

Note Cisco CallManager Extension Mobility works on phones within a single Cisco CallManager cluster only.

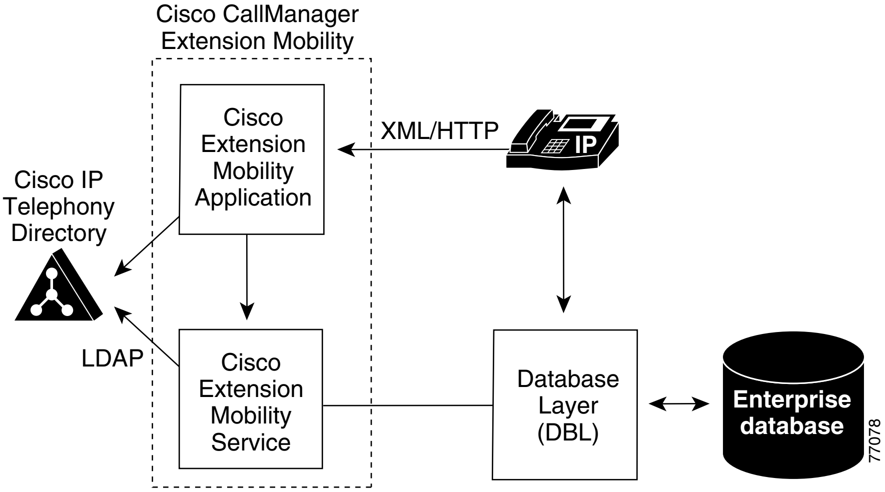
You can use Cisco CallManager Administration to start the Cisco Extension Mobility services (in Cisco CallManager Serviceability Administration), define how the features will work in your system (using the System Parameters window), and define the phone models that will support the feature (using the Device Profile Default window).

As system administrator, you configure a user device profile for each individual user. Using the Cisco CallManager User Options window, a user can access this profile and make changes, such as adding a service like Cisco Extension Mobility.

Users access Cisco CallManager Extension Mobility by pressing the Services button on a Cisco IP Phone and then entering login information in the form of a Cisco CallManager UserID and a Personal Identification Number (PIN). If a user has more than one user device profile, a prompt displays on the phone and asks the user to choose a device profile for use with Cisco CallManager Extension Mobility.

When a user logs in, the Cisco Extension Mobility application receives the XML-over-HTTP request for user authentication and verifies the information against the Cisco CallManager Directory. (See Figure 1-1.)

Figure 1-1 Cisco CallManager Extension Mobility


Cisco CallManager Extension Mobility
Cisco Extension Mobility Application
XML/HTTP
IP
Cisco IP Telephony Directory
LDAP
Cisco Extension Mobility Service
Database Layer (DBL)
Enterprise database
77078

On authentication, if the login profile matches the login device (that is, the user has a user device profile that is configured for a Cisco IP Phone Model 7960 and logs into a Cisco IP Phone Model 7960), Cisco CallManager Extension Mobility behaves the same way as it does with Cisco CallManager 3.3:

- The phone automatically reconfigures with the individual user device profile information.

  If the user has one user device profile, then the system uses this profile. If the user has more than one user device profile, the user can choose the user device profile that will be used from a list.
- The user can access all the services that the user configured on the device profile.

If that same user logs into a Cisco IP Phone model where the user does not have a configured user device profile, the login profile will not match the login device on authentication. In this scenario, the system loads the device profile default for that phone model onto the phone, and Cisco CallManager Extension Mobility works as described here:

- The system copies all device-independent configuration (that is, user hold audio hold audio source, user locale, userid, speeddials, and directory number configuration except for the setting "line setting for this device") from the user device profile to the login device.
- The system uses the device profile default for that phone model for phone template and softkey template configuration and, if the phone can support addon modules, for the addon module.
- If the phone model supports Cisco IP Phone Services and they are configured, the system copies the services from the user device profile.

For example, the following scenarios occur when a user who has a user device profile that is configured for Cisco IP Phone model 7960 logs in to a Cisco IP Phone model 7905, and the device default profile is loaded on the phone.

- The user can access the user’s hold audio source, user locale, userid, speeddials and directory number configuration. The user cannot access his phone line setting; the system configured the phone line setting from the device profile default that is configured for the Cisco IP Phone model 7905.
- The user can access the phone template and the softkey template of the Cisco IP Phone model 7905.
- The user cannot access an addon module because Cisco IP Phone model 7905 does not support it.
- The user can access Cisco IP Phone Services if they are configured for the Cisco IP Phone model 7905, but, the parameters from the subscriber services will reflect the device profile default, not the parameters that the user chose on the User Options window.

Users log out of Cisco CallManager Extension Mobility by pressing the Services button and choosing logout. If users do not log out themselves, the system will automatically log them out if you configured the Service Parameters to do so, or the next user of the phone can log out the previous user. After logout, Cisco CallManager sends the logout profile to the phone and restarts the phone.

SIP Support for Extension Mobility

Cisco CallManager Extension Mobility supports the following Cisco SIP IP Phone models:

- 7970G/7971G
- 7961G/41G and 7961GE/41GE (G = Non Gig; GE = Gig)

Additional Information

See the Related Topics, page 1-26.

Login and Logout Behavior

This section describes how login and logout works from the user's perspective. Use this information to respond to questions or problems that users may encounter.

- Cisco recommends that you direct your users to log in to their phones at the beginning of the work day. This practice ensures that the user device profile gets loaded on their phone.
- If users make changes to their profiles on the Cisco CallManager User Options window, the changes will apply until the next time that they log in.
- The system does not apply the change if the user is already logged in.
- If the User Locale that is associated with the login user or profile does not match the locale or device, after a successful login, the phone will perform a restart followed by a reset. This occurs because the phone configuration file is being rebuilt. Addon module mismatches between profile and device may have the same behavior.
- You can establish a time limit, so Cisco CallManager Extension Mobility automatically logs out users after a certain time throughout the cluster. At the Enforce Maximum Login Time, choose **True** to specify a maximum time for logins and then set the maximum login time.

  See the "Setting the Service Parameters" section on page 1-16.
- You can set the service parameter to allow for multiple logins. If you set multiple login not allowed, Cisco CallManager Extension Mobility supports only one login at a time for a user. Subsequent logins on other devices will fail until the user logs out on the first device.
- If Auto Logout is not enabled and if users forget to log out of a phone, as system administrator, you can log them out. Another user also can log them out when the second user tries to log in to that phone.
- If users are logged out of a Cisco IP Phone that has the Cisco CallManager Extension Mobility feature configured for it, depending on the logout profile, they may not be able to check voice-messaging systems from that phone until they log in. If they receive a busy signal after pressing the Messages button or any key on the touchtone key pad, they must log in before using the phone.
- Users can log in to a phone that is off the hook; however, their Cisco IP Phone will not assume their settings until they go on-hook. When they go on-hook after logging in, their phone will display a "Resetting..." message, and then their phone settings will be available from that phone.

- A user's Cisco CallManager Extension Mobility profile does not maintain ring type, contrast settings, and volume settings; users configure these settings directly on the Cisco IP Phone.
- When a Cisco CallManager Extension Mobility user logs out of a device, all Call Back services that are active on the Cisco CallManager Extension Mobility user automatically cancel.

Additional Information

See the Related Topics, page 1-26.

Login Call Flow

This section describes the flow of events for the Cisco CallManager Extension Mobility login from a system perspective. Understanding the call flow will help you troubleshoot problems that you may have with the feature.

1. A user presses the Services button on the Cisco IP Phone and requests to log in. This action invokes a URL for the Cisco Extension Mobility application.
2. The application determines the URL of the service.

   Note Cisco CallManager Extension Mobility looks up the URL in the Cisco CallManager Directory on the first instance only; the system then stores the URL as a static variable.

3. The Cisco Extension Mobility application sends a formatted XML/HTTP query to the Cisco CallManager Extension Mobility service to determine the state of the phone. The service responds in an XML format with "No one logged in."
4. The application prompts the user for UserID and PIN. The user enters the UserID and PIN and presses the Submit softkey.
5. The phone performs a HTTP request, and the application tries to authenticate the UserID and PIN.
6. If the UserID and PIN cannot be authenticated, the phone displays "Authentication Error."

   If the UserID and PIN are authenticated, the application queries the Cisco CallManager Database to get the list of device profiles that are associated with the user.
7. The directory responds with the list of the user's device profile(s). If the list has more than one entry, the phone displays the device profiles from which the user can choose.
8. When the user chooses an entry from this list (or if the list has only one entry), the application generates the XML for the service.
9. The application posts, via HTTP, the generated XML login request to the service URL (The application determined the service URL in step 2).
10. The service responds in a defined XML format to the request with a restart to load the user device profile indicating success or a failure message.
11. The application returns the correct notification to the device. The phone restarts with the user's device profile.

Additional Information

See the Related Topics, page 1-26.

Logout Call Flow

This section describes the flow of events for the Cisco CallManager Extension Mobility logout from a system perspective. Understanding the call flow will help you troubleshoot any problems that you may have with the Cisco CallManager Extension Mobility feature.

1. A user presses the Services button on the Cisco IP Phone and requests to log out. This action invokes a URL for the Cisco Extension Mobility application.
2. The application determines the URL of the service.

   Note Cisco CallManager Extension Mobility looks up the URL in the Cisco CallManager Directory on the first instance only; the system then stores the URL as a static variable.

3. The application generates the XML to query the Cisco Extension Mobility service for the current state of the device.
4. The service responds to the application with the current state of device; for example, <userID> is logged in.
5. The application prompts the user to confirm that the user wants to log out.
6. When the user presses the Yes softkey to confirm that the user wants to log out, the application generates XML for the logout operation.
7. The application posts, via HTTP, the generated XML login request to the service URL (The application determined the service URL in Step 2).
8. In the case of a successful operation, the phone will restart and load the appropriate device profile. If a failure occurs, a message gets sent to the phone.
9. The application parses the received XML and creates an XML response message.
10. The XML gets returned as a suitable notification to the device, and the phone restarts to load the original user profile or logout profile.

Additional Information

See the Related Topics, page 1-26.

System Requirements for Cisco CallManager Extension Mobility

This version of Cisco CallManager Extension Mobility requires the following software components to operate:

- Cisco CallManager 4.0 or later

Note Cisco CallManager 3.1 introduced Cisco CallManager Extension Mobility running on the Cisco Customer Response Application (CRA) 2.2 engine. With Cisco CallManager 3.3(2) or later, the Cisco CallManager Extension Mobility application and the Cisco CallManager Extension Mobility service in Cisco CallManager provide the extension mobility functionality. The feature no longer requires the Cisco CRA engine.

Note With Cisco CallManager 3.3(2) and later, Cisco CallManager Extension Mobility installs automatically on the same server with Cisco CallManager. You do not require an additional server. Cisco CallManager Extension Mobility can run on any server in a Cisco CallManager cluster.

- Netscape 4.7 or Internet Explorer 5.5 or later for Cisco CallManager Administration

With Cisco CallManager 4.0 or later, extension mobility functionality extends to most Cisco IP Phones. Check the Cisco IP Phone model documentation to verify that Cisco CallManager Extension Mobility is supported.

Note Cisco IP Phone model 7960 and Cisco IP Phone model 7960G that are running Cisco CallManager Extension Mobility may be equipped with Cisco 7914 Expansion Modules.

Additional Information

See the Related Topics, page 1-26

Interactions and Restrictions

Use the following sections to understand how Cisco CallManager Extension Mobility interacts with other Cisco CallManager services and to understand restrictions that apply to Cisco CallManager Extension Mobility:

- Interactions, page 1-8
- Restrictions, page 1-10

Interactions

The following sections describe how Cisco CallManager Extension Mobility interacts with Cisco CallManager applications:

- Cisco CallManager Services That are Running on the Same Server, page 1-8
- Bulk Administration Tool, page 1-9
- Cisco IP Manager Assistant, page 1-9
- Cisco CallManager Attendant Console, page 1-9
- Call Display Restrictions, page 1-9

Cisco CallManager Services That are Running on the Same Server

Cisco CallManager Extension Mobility can run on the same Cisco CallManager server with Cisco IP Manager Assistant (IPMA) and CDR Analysis and Reporting (CAR).

Bulk Administration Tool

You can use the Bulk Administration Tool (BAT) to add and delete several user device profiles for Cisco CallManager Extension Mobility at one time. Refer to the *Cisco CallManager Bulk Administration Guide* for more information.

Additional Information

See the Related Topics, page 1-26

Cisco IP Manager Assistant

A manager who uses Cisco CallManager Extension Mobility can simultaneously use Cisco IP Manager Assistant (IPMA). The manager logs into the Cisco IP Phone by using Cisco CallManager Extension Mobility and then chooses the Cisco IPMA service. When the IPMA service starts, the manager can access assistants and all IPMA features (such as call filtering and Do Not Disturb). For more information about Cisco IPMA, see the Cisco IP Manager Assistant With Proxy Line Support chapter.

Cisco CallManager Attendant Console

If a user logs in to or logs out of the Cisco IP Phone by using Cisco CallManager Extension Mobility while logged in to Cisco CallManager Attendant Console, the Cisco IP Phone resets and the call-control status of the attendant console goes down. Cisco CallManager Attendant Console displays a message that indicates that the attendant needs to log out and log back in if the directory numbers of the phone have changed. The user must log out of the Cisco CallManager Attendant Console. When logging back into the Cisco CallManager Attendant Console, the attendant must specify the current directory number of the phone in the Directory Number of Your Phone field of the Settings dialog box.

For more information on entering a directory number in the Cisco CallManager Attendant Console, refer to the "Configuring Cisco CallManager Attendant Console Settings" section.

Call Display Restrictions

When you enable Call Display Restrictions with Cisco CallManager Extension Mobility, Cisco CallManager Extension Mobility functions as usual: when a user is logged in to the device, the presentation or restriction of the call information depends on the user device profile that is associated with that user. When the user logs out, the presentation or restriction of the call information depends on the configuration that is defined for that phone type in the Phone Configuration window.

To use Call Display restrictions with Cisco CallManager Extension Mobility, you enable the Ignore Presentation Indicators in both the User Device Profile Configuration window (see the "Creating the Device Profile for a User" section on page 1-20) and the Phone Configuration window (see the "Subscribing Cisco IP Phones to Cisco CallManager Extension Mobility" on page 24).

For more information about the Call Display Restrictions features, refer to the Call Display Restrictions chapter.

Restrictions

The following restrictions apply to Cisco CallManager Extension Mobility:

- Cisco CallManager Extension Mobility works on phones within a single Cisco CallManager cluster only.
- Cisco CallManager Extension Mobility supports a maximum of 4500 login and logout operations per hour. Remember that these operations are sequential, not concurrent.
- The characters that display when a user logs in depend on the current locale of the phone. For example, if the phone is currently in the English locale (based on the Logout profile of the phone), the user can only enter English characters in the UserID.
- If the User Locale that is associated with the login user or profile is not the same as the locale or device, after a successful login, the phone will perform a restart followed by a reset. This occurs because the phone configuration file is being rebuilt. Addon module mismatches between profile and device may have the same behavior.
- Cisco CallManager Extension Mobility requires a physical Cisco IP Phone for login. Users of office phones that are configured with Cisco CallManager Extension Mobility cannot log in to their phones remotely.
- When a Cisco CallManager Extension Mobility user logs out of a device, all Call Back services that are active on the Cisco CallManager Extension Mobility user automatically cancel.
- You must make entries in the user ID field (the ID that you enter on the phone during Extension Mobility login) in lower-case characters.
- When a migration from Cisco CallManager Release 4.x to Cisco CallManager Release 5.0 is done, the phones will not display the last login user IDs until users log in for the first time after the migration. When the service parameter “Remember Last Login” gets set to **True**, Cisco Extension Mobility displays the previous login user ID whenever the user logs in to the phone. This gets done based on a file on the hard disk. For the migration from Release 4.x to Release 5.0, this file does not get migrated to the database; therefore, the user ID of the previous login user will not display.
- If Cisco Extension Mobility gets stopped or restarted, the system does not auto log out users who are already logged after the expiration of logout interval. For those phones, auto-logout happens only once in a day. You can manually log out these users from either the phones or from Cisco CallManager Administration.

Installing Cisco CallManager Extension Mobility for the First Time

When you install Cisco CallManager 4.0 or later, make sure that you also install the Cisco IP Telephony Locale Installer on every server in the cluster. Installing the locale installer ensures that you have the latest translated text available for user windows and phone displays. For more information, refer to the Cisco IP Telephony Locale Installer documentation.

Now perform the procedures in the “Configuring Cisco CallManager Extension Mobility” section on page 1-11.

Additional Information

See the Related Topics, page 1-26

Configuring Cisco CallManager Extension Mobility

Review the Configuration Guidelines before you configure the feature. If you are unsure how device profiles work, refer to the "Understanding Device Profiles" section on page 1-2. Then, perform the configuration procedures in the sequence that shows the"Configuration Checklist for Cisco CallManager Extension Mobility" section on page 1-13:

- Configuration Guidelines, page 1-11
- Configuration Example 1, page 1-12
- Configuration Example 2, page 1-12
- Configuration Checklist for Cisco CallManager Extension Mobility, page 1-13

Configuration Guidelines

To avoid problems with deploying Cisco CallManager Extension Mobility, be sure to follow these configuration guidelines:

- Configure a Device Profile Default for each Cisco IP Phone Model in a cluster that you want to support Cisco CallManager Extension Mobility.
- If you want to enable all phones within a Cisco CallManager cluster for Cisco CallManager Extension Mobility, do not allow the users to control these phones.
  - In this scenario, when users go to their Cisco CallManager User Options window to change their services, they must choose "Device Profiles" from the "Select a device to configure" drop-down list box. They cannot control an individual phone nor modify the settings for an individual phone.
  - As administrator, you can change the services for a phone by using Cisco CallManager Administration. After making the changes, if you update on the main window (not the popup menu), you must reset the phone for the changes to take effect. This action ensures that the new snapshot gets stored as the logout profile.

    Note If the Enterprise Parameter "Synchronization between Auto Device Profile and Phone Configuration" is set to True, the auto device profile automatically updates, and you do not need to update on the main window.
- If a particular user controls a device, for example, the user's office phone, do not allow anyone else to log in to that device.

Caution The Cisco CallManager Extension Mobility feature does not operate properly if you allow users to access another user's assigned phone.

Additional Information

See the Related Topics, page 1-26.

Configuration Example 1

In a typical Cisco CallManager Extension Mobility scenario:

- All employees represent users of Cisco CallManager Extension Mobility.
- All users have a user device profile.
- Users do not control individual phones, and they cannot modify settings for an individual phone.
- Before a user can use a phone, the user needs to log in.
- Users can access common devices, such as lobby phones, conference room phones, and cubicle phones that are meant to be shared.
- When users go to their Cisco CallManager User Options window to change services or speed dials, they can choose only their device profiles from the "Select a device to configure" drop-down menu. This method ensures that changes that users make to their services will follow them to any Cisco IP Phone after they log in.

Configuration Example 2

In another typical Cisco CallManager Extension Mobility scenario

- Each user has an assigned phone.
- Each user has a device profile that follows the user to every device to which the user logs in.
- Each user can access common devices, such as lobby phones, conference room phones, and cubicle phones that are configured to be shared.
- In this scenario, no one can use anyone else's assigned phone.

Additional Information

See the Related Topics, page 1-26.

Configuration Checklist for Cisco CallManager Extension Mobility

Perform the procedures in the order shown in Table 1-1 to configure Cisco CallManager Extension Mobility.

Summary steps in Table 1-1 point out the major tasks required to configure Cisco CallManager Extension Mobility in Cisco CallManager Administration. For a complete set of instructions, be sure to follow the procedure that is listed in the Related Procedures and Topics.

Table 1-1 Configuration Checklist for Cisco CallManager Extension Mobility

	Configuration Steps	Related Procedures and Topics
Step 1	Using Cisco CallManager Serviceability Administration, Service Activation, activate the following Cisco Extension Mobility services: • Cisco CallManager Extension Mobility • Cisco CallManager Cisco IP Phone Services **Note** To disable the extension mobility service on any node, you must first deactivate the service in Service Activation. **Note** When a change in activation or deactivation of the Cisco Extension Mobility service occurs, on any node, the database tables get updated with information that is required to build the service URLs. The database tables also get updated when the extension mobility service parameters get modified. The EMApp service handles the change notification.	*Cisco CallManager Serviceability Administration Guide*

Table 1-1 Configuration Checklist for Cisco CallManager Extension Mobility (continued)

	Configuration Steps	Related Procedures and Topics
Step 2	Create the Cisco CallManager Extension Mobility Service. Summary steps include • Choose **Device > Device Settings > Phone Services**. • Enter the service name (such as, Extension Mobility Service or EM). • Enter the following URL: http://<IP Address of Extension Mobility server>:8080/emapp/EMAppServlet?device=#DEVICENAME# **Note** If you should enter the URL incorrectly and subscribe the wrong service to the phones, you can correct the URL, save it and press **Update Subscriptions,** or correct the URL and resubscribe each phone to which the wrong service was subscribed. • Click **Save**.	Adding the Cisco CallManager Extension Mobility Service, page 1-15.
Step 3	Configure administration parameters.	Setting the Service Parameters, page 1-16
Step 4	Create a device profile default for each phone model that you want to support Cisco Extension Mobility.	Creating a Device Profile Default for Each Cisco IP Phone Model, page 1-18
Step 5	Create the device user profile for a user. Summary steps include • Choose **Device > Device Settings >Device Profile** and click **Add New**. • Enter the Device Type. • Enter the Device Profile Name; choose the phone button template and click **Save**. • Enter the directory numbers (DNs) and required information and click **Save**. Repeat for all DNs.	Creating the Device Profile for a User, page 1-20
Step 6	Associate a user device profile to a user. Summary steps include • Choose **User Management > End User** and click **Add New**; enter user information. • In Available Profiles, choose the service that you created in Step 2 and click the down arrow; this places the service that you chose in the Controlled Profiles box. • Click **Save**.	Associating a User Device Profile to a User, page 1-23

Table 1-1 Configuration Checklist for Cisco CallManager Extension Mobility (continued)

	Configuration Steps	Related Procedures and Topics
Step 7	Configure and subscribe Cisco IP Phone and user device profile to Cisco Extension Mobility. Summary steps include • Subscribe the phone and the user device profile to Cisco Extension Mobility. • Choose **Device > Phone** and click **Add New**. • On the Phone Configuration window, in Extension Information, check **Enable Extension Mobility**. • In Logout Profile, choose **Use Current Device Settings** and click **Save**.	Cisco IP Phone Configuration, *Cisco CallManager Administration Guide* Subscribing Cisco IP Phones to Cisco CallManager Extension Mobility, page 1-24

Adding the Cisco CallManager Extension Mobility Service

Add the Cisco CallManager Extension Mobility service as a new Cisco IP Phone Service. Configure a name, description, and the URL for the Cisco CallManager Extension Mobility service.

To add the Cisco CallManager Extension Mobility service, perform the following steps:

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Device Settings > Phone Services**.

Step 2 Click **Add New**.

Step 3 At the Service Name field, enter a name for the service.

The user receives this name on the phone when the user presses the Services button. Use a meaningful name; for example, Extension Mobility or EM.

Step 4 Enter the Service URL field as it displays in the following example:

http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#

where IP Address of Extension Mobility server specifies the IP Address of the Cisco CallManager where Cisco CallManager Extension Mobility Application is activated and running.

For example:

http://123.45.67.89:8080/emapp/EMAppServlet?device=#DEVICENAME#

Tip To provide redundancy for the Cisco IP Phone Service, create a Cisco IP Phone Service that uses the host name rather than the IP address. The phone functionality for softkeys and filtering, as well as the phone service, will fail over automatically in the case of a failover.

Step 5 Click **Save.**

Additional Information

See the Related Topics, page 1-26.

Setting the Service Parameters

Set the Service Parameters to define how the Cisco CallManager Extension Mobility service will work across a Cisco CallManager cluster. You can use these settings to

- Enable and define a maximum login time.
- Define the multi-login behavior; that is, whether you allow the user to log in to more than one device at a time.
- Enable "remember last user logged in."
- Clear call logs (placed, received, and missed calls) during manual Cisco CallManager Extension Mobility login and logout. Use the "Clearing call logs" service parameter to clear call logs of a previous user. This ensures privacy and prevents users of the same phone from seeing another user's calls.

Note In Cisco CallManager 4.0 or later, you no longer enable the trace directory and debug tracing for Cisco CallManager Extension Mobility in the Service Parameters window. Instead, you use Cisco CallManager Serviceability administration. Refer to the *Cisco CallManager Serviceability Administration Guide* for details about trace.

Tip Be sure that you have activated the Cisco CallManager Extension Mobility services before you perform this procedure. The service parameters will not be visible if you have not activated the services. Refer to the *Cisco CallManager Serviceability Administration Guide* for information about using the Cisco CallManager Serviceability tool, Service Activation.

To set the Service Parameters for Cisco CallManager Extension Mobility, perform the following steps:

Procedure

Step 1 From Cisco CallManager Administration, choose **System > Service Parameters**.

The Service Parameter Configuration window displays.

Step 2 From the Server drop-down menu**,** choose the server that is running the Cisco CallManager Extension Mobility service.

Step 3 From the Service drop-down menu, choose **Cisco Extension Mobility**.

A new Service Parameter Configuration window displays.

Step 4 At the Enforce Maximum Login Time field, choose **True** to specify a clusterwide maximum time for logins. After this time, the system automatically logs out the device.

Choosing False means that no clusterwide maximum time for logins exists.

The default value specifies False.

Tip To set an automatic logout, you must choose **True** in Step 4 and also specify a system maximum login time in Step 5. Cisco CallManager then uses the automatic logout service for all logins.

Step 5 If you specified True at the Maximum Login Time field in Step 4 of this procedure, specify the maximum login time in Hours:Minutes from 0:01 to 168:00 (1 minute to one week).

The default value specifies 8:00 (8 hours).

Step 6 At the Maximum Concurrent Requests field, specify the maximum number of login or logout operations that can occur simultaneously. This number prevents the Cisco CallManager Extension Mobility service from consuming excessive system resources.

Step 7 At the Multi Login Behavior field, choose one of the following responses:

- `Multiple Logins Allowed`: A user can log in to more than one device at a time.
- `Multiple Logins Not Allowed`: The second and subsequent login attempts after a user successfully logs in once will fail.
- `Auto Logout`: After a user logs in to a second device, the Cisco CallManager automatically logs the user out of the first device.

The default value specifies Multiple Logins Not Allowed.

Step 8 At the Alphanumeric Userid field, choose **True** to allow the UserID to contain alphanumeric characters. Choosing False allows the UserID to contain only numeric characters.

The default value specifies True.

Note The Alphanumeric Userid parameter applies systemwide. You can have a mix of alphanumeric and numeric userids. The system supports only userids that can be entered by using the alphanumeric keypad. The case-sensitive userid field requires the characters to be lower case.

Step 9 At the Remember last user logged in field, choose the default value, **False**.

In a typical hoteling scenario, where users can come into any office and use any phone on a temporary basis, you should set this parameter to False.

A True setting specifies that the extension mobility application remembers the user ID of the last user that logged in to the phone. Use this setting in situations where individuals use their own phone on a regular basis, and no one else uses that phone.

For example, Cisco CallManager Extension Mobility could be used to enable the types of calls that are allowed from a phone. Individuals who are not logged in and who are using their office phone can make only internal or emergency calls. But after logging in using Cisco CallManager Extension Mobility, the user can make local, long-distance, and international calls. In this scenario, only this user regularly logs in to the phone. It makes sense to set the Cisco CallManager Extension Mobility to remember the last user ID that logged in, and you would set the field to **True**. When the field is set to True, then all future logins will cause the user ID of the last successful logged in user to automatically be filled in and remembered by Cisco CallManager Extension Mobility.

Step 10 At the Clear the call log field, choose **True** to specify that the call logs are cleared during the Cisco CallManager Extension Mobility manual login/logout process.

While a user is using the Cisco CallManager Extension Mobility service on an IP phone, all calls (placed, received, or missed) appear in a call log and can be retrieved and seen on the IP phone display. To ensure user privacy by preventing other users of the same phone from seeing the call logs of the previous user, set the Clear the call log service parameter to **True**. This ensures that the call logs are cleared when a successful login/logout occurs.

Note Call logs get cleared only during manual Cisco CallManager Extension Mobility login/logout. If a Cisco CallManager Extension Mobility logout occurs due to an automatic logout or any occurrence other than a manual logout, the call logs do not get cleared.

Step 11 Click **Save**.

Tip From the Service Parameters window, you can choose another server, or you can choose to view a list of the service parameters for all servers in the cluster by choosing Parameters for All Servers from the Related Links drop-down list box and clicking **Go**; the Parameters for All Servers window displays where you can check whether any service parameters in the cluster are out of synch, or you can view just those service parameters in the cluster that have been modified.

Additional Information

See the Related Topics, page 1-26.

Creating a Device Profile Default for Each Cisco IP Phone Model

With Cisco CallManager 4.0 or later, you configure a clusterwide device profile default for each model of Cisco IP Phone that you want to support Cisco CallManager Extension Mobility. The phone takes on the device profile default whenever a user logs in to a phone model for which the user has no user device profile.

For more information on how Device Profile Defaults work, see the "Overview of Cisco CallManager Extension Mobility" section on page 1-3.

To add a device profile default for a phone model, perform the following procedure.

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Device Settings > Default Device Profile.**

The Default Device Profile Configuration window displays.

Step 2 From the Device Type drop-down list box, choose the device (such as a Cisco IP Phone) for which a profile gets created.

Step 3 Click **Next**.

Step 4 If applicable, from the Select the device protocol drop-down list box, choose a protocol.

Step 5 Click **Next**.

Step 6 From the User Hold Audio Source field, choose from the drop-down list box to specify the audio source that plays when a user initiates a hold action.

If you do not choose an audio source, Cisco CallManager uses the audio source that is defined in the device pool or, if the device pool does not specify an audio source ID, the system default.

Tip You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Service > Music On Hold**.

Step 7 At the User Locale drop-down list box, choose the locale that is associated with the phone user interface.

The user locale identifies a set of detailed information, including language and font, to support users. Cisco CallManager makes this field available only for phone models that support localization.

Note If no user locale is specified, Cisco CallManager uses the user locale that is associated with the device pool.

Note If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed **before** configuring user locale. Refer to the Cisco IP Telephony Locale Installer documentation.

Step 8 At the Phone Button Template field, choose the appropriate phone button template. The phone button template determines the configuration of the softkeys on Cisco IP Phones. Leave this field blank if the device pool contains the assigned softkey template.

Step 9 From the Privacy drop-down list box, choose **On** for each phone that wants Privacy. For more configuration information, refer to the "Barge and Privacy" section on page 8-1.

Step 10 To configure call display restrictions and ignore any presentation restriction that is received for internal calls, check the "Ignore Presentation Indicators (internal calls only)" check box.

Note Use this configuration in combination with the calling ling ID presentation and connected line ID presentation configuration at the translation pattern-level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call. For more information about call display restrictions, refer to the Call Display Restrictions chapter in the *Cisco CallManager Features and Services Guide*.

Step 11 If the phone model supports Cisco IP Phone Expansion Module 7914, Cisco CallManager displays the expansion module field.

a. At the Module 1 drop-down list box choose one or zero 7914 14-button expansion module.

b. At the Module 2 drop-down list box, choose one or zero 7914 14-button expansion module.

Step 12 To configure Multilevel Precedence and Preemption (MLPP) information, perform the following tasks:

Note Refer to the "Multilevel Precedence and Preemption" section on page 13-1 for more information.

a. At the MLPP Domain, enter a hexadecimal value for the MLPP domain that is associated with this device profile. Ensure the value is blank or a value between 0 and FFFFFF.

b. If available, the MLPP Indication setting specifies whether a device will use the capability when it places the MLPP precedence call.

From the drop-down list box, choose a setting to assign to devices that use this device profile default from the following options:

- **Default**—This device inherits its MLPP indication setting from its device pool.
- **Off**—This device does not send indication of an MLPP precedence call.
- **On**—This device does send indication of an MLPP precedence call.

Note Do not configure a device profile default with the following combination of settings: MLPP Indication is set to *Off* while MLPP Preemption is set to *Forceful*.

c. If available, the MLPP Preemption setting specifies whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting to assign to devices that use this device profile default from the following options:

- **Default**—This device inherits its MLPP preemption setting from its device pool.
- **Disabled**—This device does not preempt calls in progress when it places an MLPP precedence call.
- **Forceful**—This device preempts calls in progress when it places an MLPP precedence call.

Note Do not configure a device profile default with the following combination of settings: MLPP Indication is set to *Off* while MLPP Preemption is set to *Forceful*.

Step 13 Click **Save**.

Additional Information

See the Related Topics, page 1-26.

Creating the Device Profile for a User

The User Device Profile contains attributes such as name, description, phone template, addon modules, directory numbers, subscribed services, and speed-dial information.

Note Before proceeding, you must ensure that a device profile name and phone button template(s) are configured.

To add a default device profile for a new user of Cisco CallManager Extension Mobility, perform the following procedure.

Note If you configure BLF speed-dial buttons in the Device Profile Configuration window, a device that supports Cisco CallManager Extension Mobility can display the real-time status of the BLF speed-dial buttons after you log in to the device; that is, if the Presence Group that is applied to the device profile allows you to view the status of the presence entity. Refer to the Presence section of the *Cisco CallManager Features and Services Guide* for more details.

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Device Settings > Device Profile.**

The Find and List Device Profiles window displays.

Step 2 Click **Add New**.

The Device Profile Configuration window displays.

From the Device Type drop-down list box, choose the device type and click **Next**.

If applicable, from the Select the device protocol field, choose a protocol.

Click **Next**.

Step 3 At the User Device Profile Name field, enter a name of your choice for the device profile. You can make this text anything that describes this particular user device profile, such as “Extension Mobility.”

Step 4 At the User Locale drop-down list box, choose the locale that is associated with the phone user interface.

The user locale identifies a set of detailed information, including language and font, to support users. Cisco CallManager makes this field available only for phone models that support localization.

Note If no user locale is specified, Cisco CallManager uses the user locale that is associated with the device pool.

Note If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. Refer to the Cisco IP Telephony Locale Installer documentation.

Step 5 At the Phone Button Template field, choose the appropriate phone button template. The phone button template determines the configuration of the softkeys on Cisco IP Phones. Leave this field blank if the device pool contains the assigned softkey template.

Step 6 From the Softkey Template drop-down list box, choose a softkey template.

Step 7 From the Privacy drop-down list box, choose **On** for each phone that wants Privacy. For more configuration information, refer to the “Barge and Privacy” section on page 8-1.

Step 8 To enable the Call Display Restrictions feature, check the Ignore Presentation Indicators check box.

Note To enable the Call Display Restrictions feature, check the Ignore Presentation Indicators check box here on the User Device Profile window and also on the Phone Configuration window (see the "Subscribing Cisco IP Phones to Cisco CallManager Extension Mobility" section on page 1-24).

Step 9 If the phone model supports Cisco IP Phone 7914 Expansion Modules, Cisco CallManager displays expansion module field. At the Module 1 drop-down list box and at the Module 2 drop-down list box, choose one or zero 7914 14-button expansion module.

Note You may view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate window pops up and displays the phone buttons for that particular expansion module.

Step 10 To configure Multilevel Precedence and Preemption (MLPP) information, perform the following tasks:

Note Refer to the "Multilevel Precedence and Preemption" section on page 13-1 for more information.

a. At the MLPP Domain, enter a hexadecimal value for the MLPP domain that is associated with this device profile. Ensure the value is blank or a value between 0 and FFFFFF.

b. If available, the MLPP Indication setting specifies whether a device will use the capability when it places the MLPP precedence call.

From the drop-down list box, choose a setting to assign to devices that use this device profile default from the following options:

- **Default**—This device inherits its MLPP indication setting from its device pool.
- **Off**—This device does not send indication of an MLPP precedence call.
- **On**—This device does send indication of an MLPP precedence call.

Note Do not configure a device profile default with the following combination of settings: MLPP Indication is set to *Off* while MLPP Preemption is set to *Forceful*.

c. If available, the MLPP Preemption setting specifies whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting to assign to devices that use this device profile default from the following options:

- **Default**—This device inherits its MLPP preemption setting from its device pool.
- **Disabled**—This device does not preempt calls in progress when it places an MLPP precedence call.
- **Forceful**—This device preempts calls in progress when it places an MLPP precedence call.

Note Do not configure a device profile default with the following combination of settings: MLPP Indication is set to *Off* while MLPP Preemption is set to *Forceful*.

Step 11 From the Login User Id drop-down list box, choose a user ID.

Click **Save**.

The page refreshes.

Step 12 From the Association Information section, click the Add a new DN link.

Step 13 At the Directory Number field, enter the directory number and click **Save**.

Refer to "Directory Number Configuration Settings" in the *Cisco CallManager Administration Guide* for field descriptions.

Step 14 The following prompt displays: Changes to Line or Directory Number settings require restart.

Click **Reset** and follow the prompts.

Additional Information

See the Related Topics, page 1-26.

Associating a User Device Profile to a User

You associate a User Device Profile to a user in the same way that you associate a physical device. For more details, refer to the "Adding a New User" in the *Cisco CallManager Administration Guide*.

Tip You can use the Bulk Administration Tool (BAT) to add and delete several user device profiles for Cisco CallManager Extension Mobility at one time. Refer to the *Cisco CallManager Bulk Administration Guide* for more information.

To associate a user device profile to a user for Cisco CallManager Extension Mobility, follow these steps:

Procedure

Step 1 From Cisco CallManager Administration, choose **User Management> End User**.

Step 2 Click **Add New**.

Step 3 Enter the appropriate settings as described in "End User Configuration Settings" in the *Cisco CallManager Administration Guide*.

Step 4 To save your changes and add the user, click **Save**.

Note To choose an existing end user, click **Find** and then choose the end user to whom you want to associate a user device profile. Refer to "Finding an End User" in the *Cisco CallManager Administration Guide*.

Additional Information

See the Related Topics, page 1-26.

Subscribing Cisco IP Phones to Cisco CallManager Extension Mobility

Prerequisite

You must configure the Cisco IP Phones in Cisco CallManager before you subscribe the phones to Cisco CallManager Extension Mobility. To configure the phones, refer to the "Cisco IP Phone Configuration" section in the Cisco CallManager Administration Guide.

For a review of device profiles, refer to the "Understanding Device Profiles" section on page 1-2.

To subscribe to the Cisco CallManager Extension Mobility service, perform the following procedure.

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Phone**.

Step 2 Click **Add New**.

Note You can also search and update a configured phone as described in "Finding a Phone" in the *Cisco CallManager Administration Guide*.

The Add a New Phone window displays.

Step 3 From the Phone Type drop-down list box, choose the phone type to which you want to subscribe extension mobility and click **Next**.

Step 4 From the Select the device protocol drop-down list box, choose the protocol of the phone and click **Next**.

Step 5 In Extension Information, check the Enable Extension Mobility check box.

Note For descriptions of all fields, refer to "Phone Configuration Settings" in the *Cisco CallManager Administration Guide*.

Step 6 From the Log Out Profile drop-down list box, choose the type of profile that you want the phone to use for extension mobility.

To choose a specific configured profile, follow the steps in Step 7; otherwise, proceed to Step 11.

Step 7 From the Log Out Profile drop-down list box, choose Select a User Device Profile.

Note You can either choose Select a User Device Profile, or Use Current Device Settings. If you choose Use Current Device Settings, then an automated device profile will be used when logout executes.

The User Device Profile Configuration window displays.

Step 8 From the User Device Profile Name drop-down list box, choose a user device profile.

Step 9 Click **Close and go Back**.

This action specifies the device profile that the device uses when no one is logged in to the device that is using Cisco CallManager Extension Mobility. When a logout executes, the Autogenerated Device Profile (the default device profile) replaces the current configuration (the User Device Profile).

Note Cisco strongly recommends that you use the Autogenerated Device Profile and not assign a user device profile as the default device profile.

The remaining fields show the current device information regarding the login status of the device: Log in UserID, Log In Time, Log Out Time.

Step 10 On the Cisco CallManager Phone Configuration window, to enable the Call Party Restrictions feature, check the Ignore Presentation Indicators check box.

Note To enable the Call Display Restrictions feature, check the Ignore Presentation Indicators check box here on the Phone Configuration window and also on the User Device Profile window (see the "Creating the Device Profile for a User" section on page 1-20). For information about this feature, refer to the Call Display Restrictions chapter.

Step 11 Click **Save**.

You must now subscribe the extension mobility IP phone service to both the device profile that you created in the "Creating a Device Profile Default for Each Cisco IP Phone Model" section on page 1-18 and the IP phone target device.

Step 12 To subscribe extension mobility to the IP phone, go to the Related Links drop-down list box in the upper, right corner of the window and choose Subscribe/Unsubscribe Services; then, click **Go**.

A separate Subscribed Cisco IP Phone window displays.

Step 13 From the Select a Service drop-down list box, choose the service to which you want this IP phone to subscribe.

Step 14 Click **Next**.

Step 15 Click **Subscribe**.

Step 16 The new service(s) displays under Subscribed Services.

Step 17 Click **Save**.

Step 18 Repeat the procedure for each service to which you want this IP phone to subscribe.

Step 19 To unsubscribe a service, click **Unsubscribe** and **Save**.

Note To subscribe/unsubscribe services to a device profile, see the "Creating a Device Profile Default for Each Cisco IP Phone Model" section on page 1-18

You have now configured Cisco CallManager Extension Mobility.

Additional Information

See the Related Topics, page 1-26.

Providing Information to Cisco CallManager Extension Mobility Users

After you have configured the system for Cisco CallManager Extension Mobility, provide your phone users with the following information:

- Notification of feature availability and the phone models that support Cisco CallManager Extension Mobility. Include the name that you have given the Cisco CallManager Extension Mobility feature (for example, extension mobility). In addition, notification of changes with respect to activation and deactivation of extension mobility service on any node in the Cisco CallManager cluster.
- User password, UserID, and PIN
- URL for the Cisco CallManager User Options window for the user to change user password and PIN

Note Be aware that user passwords and PINs can only contain characters that the IP phones support: the digits 0 - 9 and their corresponding letters; the asterisk (*); and the octothorpe or pound sign (#).

- Their phone model user guide that contains a Cisco CallManager Extension Mobility overview and instructions on logging in, logging out, and troubleshooting the feature.
- The *Customizing Your Cisco IP Phone on the Web* document that contains information on using their Cisco IP Options window.
- Description of the feature login and logout behavior that you defined in the "Setting the Service Parameters" section on page 1-16.

Additional Information

See the Related Topics, page 1-26.

Related Topics

- Introducing Cisco CallManager Extension Mobility, page 1-1
- Overview of Cisco CallManager Extension Mobility, page 1-3
- Login and Logout Behavior, page 1-5
- Login and Logout Behavior, page 1-5
- Logout Call Flow, page 1-7
- Login Call Flow, page 1-6
- System Requirements for Cisco CallManager Extension Mobility, page 1-7
- Interactions and Restrictions, page 1-8
- Installing Cisco CallManager Extension Mobility for the First Time, page 1-10
- Configuring Cisco CallManager Extension Mobility, page 1-11
- Configuration Example 1, page 1-12

- Configuration Example 2, page 1-12
- Configuration Checklist for Cisco CallManager Extension Mobility, page 1-13
- Adding the Cisco CallManager Extension Mobility Service, page 1-15
- Setting the Service Parameters, page 1-16
- Subscribing Cisco IP Phones to Cisco CallManager Extension Mobility, page 1-24
- Providing Information to Cisco CallManager Extension Mobility Users, page 1-26

Device Profiles

- Understanding Device Profiles, page 1-2
- Associating a User Device Profile to a User, page 1-23
- Creating the Device Profile for a User, page 1-20

Cisco IP Manager Assistant With Proxy Line Support

The Cisco IP Manager Assistant (Cisco IPMA) feature enables managers and their assistants to work together more effectively. Cisco IPMA supports two modes of operation: proxy line support and shared line support. The Cisco IPMA service supports both proxy line and shared line support simultaneously in a cluster. For information about Cisco IPMA with shared line support, see Cisco IP Manager Assistant With Shared Line Support.

The feature comprises a call-routing service, enhancements to phone capabilities for the manager and the assistant, and assistant console interfaces that are primarily used by the assistant.

The service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets on the basis of preconfigured call filters. The manager can change the call routing dynamically; for example, by pressing a softkey on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Cisco CallManager users comprise managers and assistants. The routing service intercepts manager calls and routes them appropriately. An assistant user handles calls on behalf of a manager.

This chapter provides the following information about Cisco IPMA:

- Introducing Cisco IPMA, page 2-1
- System Requirements for Cisco IPMA with Proxy Line Support, page 2-6
- Interactions and Restrictions, page 2-7
- Installing and Activating Cisco IPMA, page 2-10
- Configuring Cisco IPMA with Proxy Line Support, page 2-10
- Providing Information to Cisco IPMA Managers and Assistants, page 2-31
- Related Topics, page 2-33

Introducing Cisco IPMA

The following sections provide information about the Cisco IPMA feature:

- Cisco IPMA Architecture Overview, page 2-2
- Cisco IPMA Database Access Architecture, page 2-5
- Manager Interfaces, page 2-5
- Assistant Interfaces, page 2-5

- Softkeys, page 2-5
- Manager Assistant Administration Interface, page 2-6

Cisco IPMA Architecture Overview

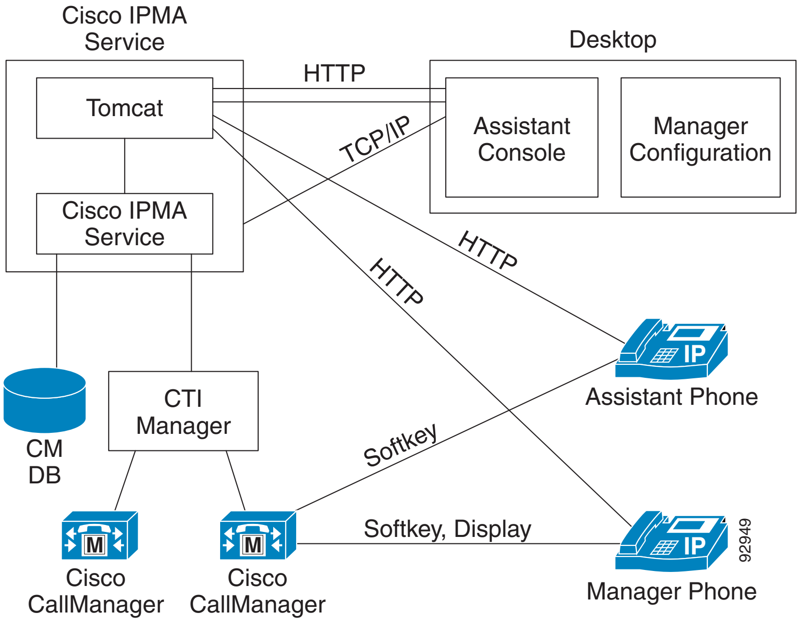
The Cisco IPMA feature architecture comprises the Cisco IPMA service, the assistant console interfaces, and the Cisco IP Phone interfaces. See Figure 2-1.

Cisco IPMA service routes calls that are presented to a CTI route point that is defined in the Cisco IP Manager Assistant service parameters. See the "Setting the Service Parameters for Cisco IPMA" section on page 2-18.

Additional Information

See the "Related Topics" section on page 2-33.

Figure 2-1 Cisco IPMA Architecture



Cisco IPMA Service

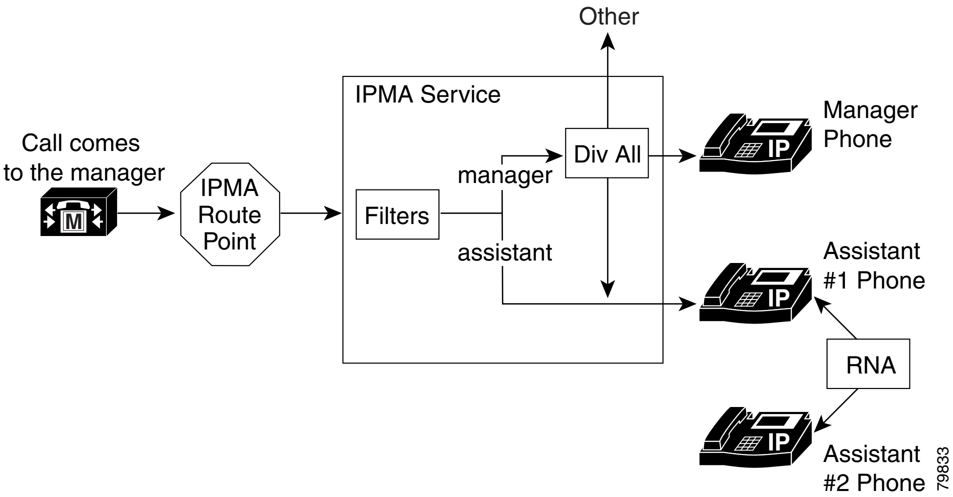
Cisco Tomcat loads the Cisco IPMA service, a servlet. Cisco Tomcat gets installed at Cisco CallManager installation.

The Cisco IPMA service gets installed on all Cisco CallManager servers in a cluster. After installation, the administrator activates the service from Serviceability, which automatically starts IPMA. When started, the IPMA service checks to see whether it is one of the IPMA servers that is configured in the clusterwide service parameter, Cisco IPMA Server (Primary) IP Address. If it is, the IPMA service attempts to become the active Cisco IPMA service. Currently, a Cisco CallManager cluster supports only one active Cisco IPMA service.

The Cisco IPMA service performs the following tasks:

- Hosts the HTTP services that run on the manager phone.
- Hosts the web pages that the manager uses for configuration.
- Contains the routing logic that applies filters on an incoming call for a manager. See Figure 2-2.
- Communicates to a Cisco CallManager cluster through the Cisco CTIManager for third-party call control. Cisco IPMA requires only one CTI connection for all users in a cluster.
- Accesses data from the database.
- Supports the Assistant Console application.

Figure 2-2 Cisco IPMA Routing Logic for Proxy Line Support

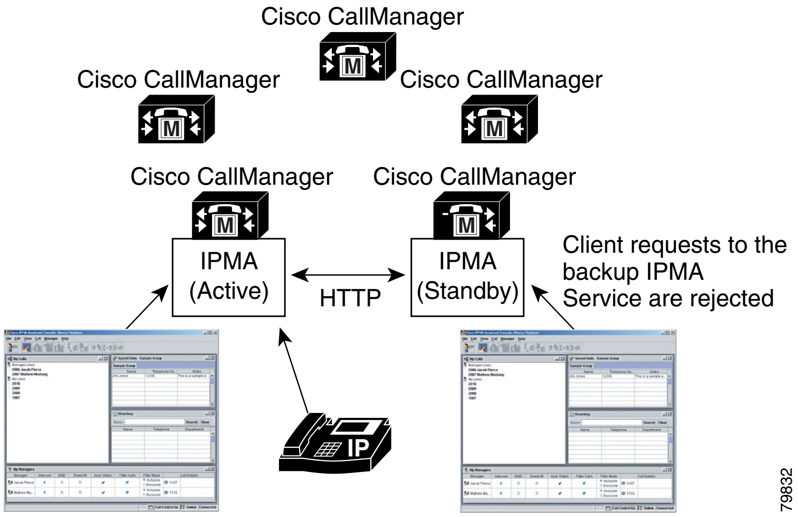


Cisco IPMA provides support for redundancy. To achieve redundancy, you must configure a second Cisco IPMA service in the same cluster.

IPMA implements redundancy by using an active/standby server model. At any time, only one IPMA server remains active and servicing all assistant console applications and phones. The other server stays in a standby mode and will detect failures on the active server. When it detects a failure, the backup server takes over and becomes the active server. All connections that were active get restored on the new server, and service continues uninterrupted to the users.

If the active server fails, the Assistant Console application fails over automatically to the backup server. The Cisco IPMA Assistant Console Heartbeat Interval service parameter (see the "Setting the Service Parameters for Cisco IPMA" section on page 2-18) determines the time that the application takes to detect failure. A shorter heartbeat interval leads to faster failover. See Figure 2-3.

Figure 2-3 Cisco IPMA Redundancy



The Cisco IPMA service includes built-in security to help prevent unauthorized access to its services. The user ID and password that are collected at the assistant console get encrypted before they are sent over the network. The Assistant Console blocks nonauthorized users who are posing as assistants.

Assistant Console Interface

Cisco IPMA supports the following assistant console interfaces for managers and assistants:

- Assistant Console (used for call control, log on, assistant preferences, monitoring managers call activity, keyboard shortcuts)
- Manager configuration (used to configure send all calls target, immediate divert target, and filters)

Administrators use Cisco CallManager Administration, End User Configuration, to configure Cisco IPMA for managers and assistants. See "Manager Assistant Administration Interface" section on page 2-6.

Cisco CallManager makes all Cisco IPMA manager features available through the Cisco IP Phone, except manager configuration, which is available by using a browser. Assistants use the Cisco IP Phone and the assistant console application. See "Manager Interfaces" section on page 2-5 and "Assistant Interfaces" section on page 2-5.

For more information about how to use the Cisco IPMA features, refer to the *Cisco IP Manager Assistant User Guide*.

Cisco IP Phone Interface

Assistants use softkeys to access the Cisco IPMA features, and managers use softkeys and the Cisco IP Phone Services button. For more information about how to use the Cisco IPMA Phone features, refer to the *Cisco IP Manager Assistant User Guide*.

See "Manager Interfaces" section on page 2-5 and "Assistant Interfaces" section on page 2-5.

Cisco IPMA Database Access Architecture

The database stores all Cisco IPMA configuration information. When the manager or assistant logs in, the IPMA service retrieves all data that is related to the manager or assistant from the database and stores it in memory.

Manager Interfaces

The manager phone makes all manager features available with the exception of Manager Configuration. Cisco IPMA automatically logs a manager into the IPMA service when the Cisco IPMA service starts.

The manager can change selected assistants by using the Cisco IP Phone Services button.

The manager accesses the Cisco IPMA features Assistant Watch, Do Not Disturb, Immediate Divert, Intercept Call, and Transfer to Voice Mail from the Cisco IP Phone softkeys.

The state of the features Assistant Watch, Do Not Disturb, Divert All Calls, and Filtering displays in the Status Window on the Cisco IP Phone.

You can enable filtering and choose filter mode by using the Cisco IP Phone Services button. Configuration of the filters occurs by using Manager Configuration. You can access the Manager Configuration on the assistant console by using a web browser (see the "Manager Configuration" section on page 2-32).

Refer to the *Cisco IP Manager Assistant User Guide* for more information.

Assistant Interfaces

The assistant accesses the Cisco IPMA features by using the Assistant Console application and the Cisco IP Phone. The Assistant Console, an application, provides call-control functions such as answer, divert, transfer, and hold. The assistant uses the Assistant Console to log on and log off, to set up assistant preferences, and to display the manager configuration window that is used to configure manager preferences.

The Assistant Console displays the assistant lines and the manager proxy lines. A proxy line specifies a phone line that appears on the assistant Cisco IP Phone. Assistants use the proxy lines to manage calls that are intended for a manager. For more information on setting up proxy lines, see the "Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant" section on page 2-28.

When the assistant logs in from the Assistant Console, the softkeys Immediate Divert and Transfer to Voice Mail become active for the proxy lines. Refer to the *Cisco IP Manager Assistant User Guide* for more information.

Softkeys

The Cisco IPMA feature supports softkeys such as Immediate Divert, Transfer to Voice Mail, and Do Not Disturb on the Cisco IP Phone. Softkeys appear in their appropriate call state; for example, Transfer to Voice Mail does not appear if no active calls exist.

Cisco IPMA supports the following softkey templates:

- Standard IPMA Manager—Supports manager for proxy mode
- Standard IPMA Shared Mode Manager—Supports manager for shared mode
- Standard IPMA Assistant—Supports assistant in proxy or shared mode

Additionally, the system makes call-processing (such as hold and dial) softkeys available with the Standard User template. The administrator configures the appropriate softkey template for the devices that managers and assistants use.

Note The default process assigns call-processing softkey templates to devices.

Administrators can create custom softkey templates in addition to using the standard softkey templates that are included in Cisco CallManager. Use Softkey Template configuration in Cisco CallManager Administration to associate softkey templates with Cisco IPMA devices and to create custom softkey templates. See Softkey Template Configuration in the *Cisco CallManager Administration Guide*.

Manager Assistant Administration Interface

The administrator uses the End User Configuration window in Cisco CallManager Administration to configure the manager and assistant. The administrator chooses the device for the manager and assistant, chooses an incoming intercom line for the manager and assistant, and assigns a proxy line for a manager on the assistant phone.

See the "Manager and Assistant Configuration" section on page 2-24.

System Requirements for Cisco IPMA with Proxy Line Support

Cisco IPMA with proxy line support requires the following software components to operate:

- Cisco CallManager 5.0
- Microsoft Internet Explorer or Netscape Navigator:
  - Cisco IPMA administration (using Cisco CallManager Administration) supports Microsoft Internet Explorer (IE) 6.0 or later and Netscape 7.1 or later.
  - The Assistant Console application installation program supports Microsoft Internet Explorer (IE) 6.0 or later and Netscape 7.1 or later. (See the "Interactions and Restrictions" section on page 2-7 for more information.)
  - The Assistant Console application supports Microsoft Windows 2000 and Microsoft Windows XP.
  - The Manager Configuration application supports Microsoft Internet Explorer (IE) 6.0 or later.
- Bulk Administration Tool (BAT) if bulk adding of managers and assistants is planned.

The following SCCP phones support Cisco IPMA:

- Cisco IP Phone model 7970/71
- Cisco IP Phone model 7960/61
- Cisco IP Phone model 7940/41 (see the "Restrictions" section on page 2-9)

Note Cisco IP Phone model 7960/61 and 7970/71 that are running Cisco IPMA may be equipped with a Cisco model 7914 Expansion Module.

Because Cisco IPMA is installed automatically on the same server with Cisco CallManager, you do not require an additional server.

Interactions and Restrictions

The following sections describe the interactions and restrictions for Cisco IPMA with proxy line support:

- Interactions, page 2-7
- Restrictions, page 2-9

Interactions

The following sections describe how Cisco IPMA with proxy line support interacts with Cisco CallManager applications and call processing:

- Bulk Administration Tool, page 2-7
- Extension Mobility, page 2-7
- Reporting Tools, page 2-8
- Multilevel Precedence and Preemption (MLPP), page 2-9
- Time-of-Day Routing, page 2-9

Bulk Administration Tool

The administrator can use the Bulk Administration Tool (BAT) to add many users (managers and assistants) at once instead of adding users individually. Refer to the *Cisco CallManager Bulk Administration Guide* for more information.

Additional Information

See the "Related Topics" section on page 2-33.

Extension Mobility

A manager who uses the Cisco CallManager Extension Mobility feature can simultaneously use Cisco IPMA. The manager logs into the Cisco IP Phone by using extension mobility and then chooses the Cisco IPMA service. When the IPMA service starts, the manager can access assistants and all IPMA features (such as call filtering and Do Not Disturb).

To have access to Cisco CallManager Extension Mobility with IPMA, the administrator checks the Mobile Manager check box in the Cisco IPMA Manager Configuration window in Cisco CallManager Administration (which is accessed from the End User Configuration window). See the "Configuring a Manager and Assigning an Assistant for Proxy Line Mode" section on page 2-25. For more information about configuring device profiles, see Configuring a New User Device Profile in the *Cisco CallManager Administration Guide*. For more information about Cisco CallManager Extension Mobility, see Chapter 1, "Cisco CallManager Extension Mobility."

Reporting Tools

Cisco IPMA provides statistical information in the CDR Analysis and Reporting (CAR) tool and provides a summary of changes to configurations in a change log. The following sections describe these reporting tools.

CDR Analysis and Reporting

Cisco IPMA supports call-completion statistics for managers and assistants and inventory reporting for managers and assistants. The CDR Analysis and Reporting (CAR) tool supports call-completion statistics. Cisco CallManager Serviceability supports inventory reporting. Refer to the *Cisco CallManager Serviceability System Guide*, the *Cisco CallManager Serviceability Administration Guide*, and the *CDR Analysis and Reporting Administration Guide* for more information.

IPMA_ChangeLog

The administrator can view a summary of changes that are made to the Manager or Assistant Configurations. A manager can change defaults by accessing the Manager Configuration from a URL.

An assistant can change the manager defaults from the Assistant Console.

Note Refer to the *Cisco IP Manager Assistant User Guide* for information about the URL and Manager Configuration.

When changes are made, the information gets sent to a log file that is called ipma_changeLogxxx.log. The log file resides on the server that runs the IPMA service at the following location:

file get activelog tomcat/logs/ipma/log4j

The administrator can download this file from the server by using the Trace Collection Tool in the Serviceability Real-Time Monitoring Tool (RTMT). Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

The log file contains the following fields:

- LineNumber—The line in the log file with information about changes
- TimeStamp—The time that the configuration changed
- for Manager/Assistant—Designation of whether the change is for the manager or the assistant
- for Userid—The userid of the manager or assistant that is being changed
- by Manager/Assistant—Designation of whether the manager or the assistant made the change
- by Userid—The userid of the manager or assistant who made the change
- Parameter Name—What changed; for example, divert target number
- Old Value—The value of the information before the change
- New Value—The value of the information after the change

Because the information in the log file is comma delimited, the administrator can open the log file by using a spreadsheet application such as Microsoft Excel. Use the following procedure to save the log file contents to the Microsoft Excel application.

Procedure

Step 1 Start the Microsoft Excel application.

Step 2 To open the ConfigChange*.log file, choose **File > Open**.

Step 3 Choose the Original data type, file type as Delimited, and click **Next**.

Step 4 Choose Delimiters as Comma and click **Next**.

Step 5 When complete, click **Finish**.

Multilevel Precedence and Preemption (MLPP)

The following points describe the interactions between Cisco IPMA with proxy line support and MLPP:

- IPMA preserves call precedence in the handling of calls. For example, when an assistant diverts a call to a manager, IPMA preserves the precedence of the call.
- Filtering of precedence calls occurs in the same manner as all other calls. The precedence of a call will not affect whether a call is filtered.
- Because IPMA does not perceive the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.

Time-of-Day Routing

Time-of-Day routing routes calls to different locations based on the time that the call gets made; for example, during business hours, calls get routed to a manager office, and after hours, the calls go directly to voice-messaging service.

Partitions specify the time schedule and time zone that Time-of-Day routing uses. IPMA partitions and partitions in IPMA calling search spaces support Time-of-Day routing.

For more information about Time-of-Day routing, see Time-of-Day Routing in the *Cisco CallManager System Guide*.

Restrictions

The following restrictions apply to Cisco IPMA:

- Cisco IPMA does not support Cisco IP SIP phones.
- One manager can have up to 10 assigned assistants.
- One assistant can support up to 33 managers (if each manager has one IPMA-controlled line).
- Cisco IPMA supports up to 1024 managers and 1024 assistants per Cisco CallManager cluster.
- Cisco IPMA Assistant Console does not support hunt groups/queues.
- Cisco IPMA Assistant Console does not support record and monitoring.
- Cisco IPMA Assistant Console does not support onhook transfer (the ability to transfer a call by pressing the Transfer softkey and going onhook to complete the transfer).
- Cisco IPMA Assistant Console does not support the one-touch Call Pickup feature.
- Cisco IP Phone model 7940 supports only two lines or speed-dial buttons.

- To install the Assistant Console application on a computer with Microsoft IE version 6 on Windows XP, install the Microsoft Java Virtual Machine (JVM) with Windows XP Service Pack 1 before the Assistant Console installation.

Installing and Activating Cisco IPMA

Cisco Tomcat loads the Cisco IPMA, a servlet. Cisco Tomcat gets installed and started at Cisco CallManager installation. For more information, see the "Cisco IPMA Service" section on page 2-2.

The administrator performs three steps after installation to make Cisco IPMA available for system use:

1. Use Cisco CallManager Serviceability Service Activation, located on the Tools menu, to activate the Cisco IP Manager Assistant service. Refer to the *Cisco CallManager Serviceability Administration Guide*.
2. Configure the applicable service parameters for the Cisco IP Manager Assistant service. See the "Setting the Service Parameters for Cisco IPMA" section on page 2-18.
3. Use Serviceability Control Center Feature Service web page to stop and start the Cisco IPMA service. See the "Starting the Cisco IPMA Service" section on page 2-20.

Note If the managers and assistants will require Cisco IPMA features to display (on the phone and assistant console) in any language other than English, verify that the locale installer is installed before configuring Cisco IPMA. Refer to the Cisco IP Telephony Locale Installer documentation.

Configuring Cisco IPMA with Proxy Line Support

For successful configuration of Cisco IPMA, review the steps in the configuration checklist, perform the system, user, and device configuration requirements, and configure the managers and assistants.

Note Cisco IPMA with proxy line support coexists in the same Cisco CallManager cluster with Cisco IPMA with shared line support. For configuration information about shared line support, see Configuring Cisco IPMA with Shared Line Support.

The following sections provide configuration information:

- Configuration Checklist for Cisco IPMA with Proxy Line Support, page 2-11
- System Configuration with Proxy Line Support, page 2-13
- Setting the Service Parameters for Cisco IPMA, page 2-18
- Security Considerations, page 2-20
- Starting the Cisco IPMA Service, page 2-20
- Cisco IP Phone Service Configuration, page 2-20
- Manager and Assistant Phone Configuration, page 2-21
- Manager and Assistant Configuration, page 2-24

Configuration Checklist for Cisco IPMA with Proxy Line Support

Table 2-1 shows the logical steps for configuring the Cisco IP Manager Assistant feature in Cisco CallManager.

Before You Begin

The information in the checklist assumes that you have already configured the phones and the users and have associated the devices to the users. Refer to Adding an End User, Associating Devices to an End User, and Configuring Cisco IP Phones in the *Cisco CallManager Administration Guide*.

Table 2-1 Cisco IP Manager Assistant Configuration Checklist with Proxy Line Support

Configuration Steps		Related Procedures and Topics
Step 1	Using Cisco CallManager Serviceability, Service Activation, activate Cisco IP Manager Assistant service.	*Cisco CallManager Serviceability Administration Guide*
Step 2	Configure system administration parameters: • Add three partitions. • Add two calling search spaces. • Add the CTI route point for IPMA. You can have only one route point per server. • Configure IPMA service parameters. **Tip** To automatically configure these system administration parameters, use the Cisco IPMA Configuration Wizard. For more information, see the "Cisco IPMA Configuration Wizard" section on page 2-13.	Calling Search Space and Partitions, page 2-16 Configuring a Partition, *Cisco CallManager Administration Guide* Configuring a Calling Search Space, *Cisco CallManager Administration Guide* Cisco IPMA Route Point, page 2-17 Configuring a CTI Route Point, *Cisco CallManager Administration Guide* Cisco IPMA Configuration Wizard, page 2-13 Setting the Service Parameters for Cisco IPMA, page 2-18 Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 3	• Configure the application user CAPF profile (optional). • Configure IPMA service parameters for security (optional).	Setting the Service Parameters for Cisco IPMA, page 2-18 Security Considerations, page 2-20
Step 4	Using the Serviceability Control Center Feature Services, stop and start the Cisco IPMA service.	Starting the Cisco IPMA Service, page 2-20
Step 5	Configure phone parameters: • Add IPMA service as a Cisco IP Phone service. • Configure Cisco IP Phone.	Cisco IP Phone Service Configuration, page 2-20 Configuring a Cisco IP Phone Service, *Cisco CallManager Administration Guide* Configuring Phone Button Templates, *Cisco CallManager Administration Guide*
Step 6	Configure manager and assistant Cisco IP Phone parameters: • Set up manager phone. • Set up assistant phone.	Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*

Table 2-1 Cisco IP Manager Assistant Configuration Checklist with Proxy Line Support (continued)

Configuration Steps		Related Procedures and Topics
Step 7	Configure manager phone settings: • Assign a softkey template. • Add a primary line. • Set up voice-mail profile on primary line. • Add incoming intercom line. • Add speed dial for outgoing intercom targets. • Subscribe to Cisco IP Phone Service, Cisco IPMA. • Set user locale. • Reset the phone. **Tip** To automatically configure some of the manager phone settings, choose the automatic configuration check box on the Cisco IPMA Manager Configuration window. For more information, see the "Manager Phones" section on page 2-22.	Manager and Assistant Phone Configuration, page 2-21 Finding a Phone, *Cisco CallManager Administration Guide* Deleting a Phone, *Cisco CallManager Administration Guide* Directory Number Configuration Overview, *Cisco CallManager Administration Guide* Configuring Speed-Dial Buttons, *Cisco CallManager Administration Guide* Cisco IP Phone Service Configuration, page 2-20 Configuring Cisco IP Phone Services, *Cisco CallManager Administration Guide* Resetting a Phone, *Cisco CallManager Administration Guide*
Step 8	Configure assistant phone settings: • Assign a softkey template. • Add a Cisco 14-button expansion module (7914) (optional). • Assign the Standard IPMA Assistant phone button template. • Add a primary line. • Add proxy lines for each configured manager. Add a voice-mail profile that is the same as the voice-mail profile on the manager primary line. • Add incoming intercom line. • Add speed dial to the incoming intercom line for each configured manager. • Set user locale. • Reset the phone. **Tip** To automatically configure some assistant phone settings, choose the Automatic Configuration check box on the Cisco IPMA Assistant Configuration window. For more information, see the "Assistant Phones" section on page 2-23.	Manager and Assistant Phone Configuration, page 2-21 Finding a Phone, *Cisco CallManager Administration Guide* Deleting a Phone, *Cisco CallManager Administration Guide* Directory Number Configuration Overview, *Cisco CallManager Administration Guide* Configuring Speed-Dial Buttons, *Cisco CallManager Administration Guide* Resetting a Phone, *Cisco CallManager Administration Guide*
Step 9	Configure Cisco IP Manager Assistant application: • Create a new manager. • Configure lines for manager. • Assign an assistant to a manager. • Configure lines for the assistant.	Configuring a Manager and Assigning an Assistant for Proxy Line Mode, page 2-25 Deleting Cisco IPMA Information from the Manager, page 2-26 Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant, page 2-28

Table 2-1 Cisco IP Manager Assistant Configuration Checklist with Proxy Line Support (continued)

Configuration Steps		Related Procedures and Topics
Step 10	Configure the dial rules for the assistant.	Dial Rules Configuration, page 2-31
Step 11	Install the Assistant Console application.	Installing the Assistant Console Application, page 2-32
Step 12	Configure the manager and assistant console applications.	*Cisco IP Manager Assistant User Guide*

System Configuration with Proxy Line Support

Because the Cisco IPMA service intercepts calls that are made to managers who are using proxy line mode, it requires configuration of partitions, calling search spaces, and route points. For more information on configuring Cisco IPMA, see the "Configuration Checklist for Cisco IPMA with Proxy Line Support" section on page 2-11.

You must perform the following configurations before you configure devices and users for Cisco IPMA:

- Calling Search Space and Partitions, page 2-16
- Cisco IPMA Route Point, page 2-17

Cisco IPMA provides a one-time-use configuration wizard that helps the administrator configure partitions, calling search spaces, a route point, and the IPMA phone service. The Cisco IPMA Configuration Wizard also creates the Cisco IP Manager Assistant service parameters in the IPMA Device Configuration Defaults section. For more information on the Cisco IPMA Configuration Wizard, see the "Cisco IPMA Configuration Wizard" section on page 2-13.

Note This document provides specific information about IPMA configuration. For more information about configuring Calling Search Spaces, Partitions, and CTI Route Points, refer to the *Cisco CallManager Administration Guide*.

Cisco IPMA Configuration Wizard

With the Cisco IPMA Configuration Wizard, IPMA configuration takes less time and eliminates errors. The partitions, calling search spaces, and route point automatically get created when the administrator successfully runs and completes the configuration wizard. The wizard also creates BAT templates for the IPMA manager phone, the IPMA assistant phone, and all other user phones. The administrator can use the BAT templates to configure the managers, assistants, and all other users. Refer to the *Cisco CallManager Bulk Administration Guide*.

Note The Cisco IPMA Configuration Wizard only creates the Cisco IP Manager Assistant service parameters in the IPMA Device Configuration Defaults section of the Service Parameters Configuration window. You must enter the remaining service parameters manually. For service parameter information, see the "Setting the Service Parameters for Cisco IPMA" section on page 2-18.

The Cisco IPMA Configuration Wizard provides windows for each configuration parameter. The windows provide the administrator with preconfigured information. If the administrator prefers to use other configuration information (for example, partition names), the administrator can change the preconfigured information to the appropriate information.

Perform the following procedure to configure the Cisco IPMA system parameters by using the Cisco IPMA Configuration Wizard.

Before You Begin

Ensure that the configuration wizard runs from the same server (the Cisco CallManager server) as the Bulk Administration Tool (BAT).

Procedure

Step 1 From the Cisco CallManager Administration window, choose **Application > Cisco IPMA Configuration Wizard**.

The Cisco IPMA Configuration Wizard Overview window displays and provides a description of the configuration wizard process.

Note You can use the Cisco IPMA Configuration Wizard only once in a Cisco CallManager cluster configuration. The feature verifies the number of times that the configuration wizard has been run (zero or 1). If the configuration wizard has been run once, the summary window automatically displays. The summary window displays the details and status of the configuration wizard that was previously run. If the configuration has not been run, the configuration process continues.

Step 2 To begin the IPMA wizard process, click the **Next** button.

The Partition for Managers window displays.

Step 3 Enter a name in the partition name field and provide a description; otherwise, use the default partition name and description.

Step 4 Click the **Next** button.

The Partition for IPMA window displays.

Step 5 Enter a name in the partition name field and provide a description; otherwise, use the default partition name and description.

Step 6 Click the **Next** button.

The Partition for All Users window displays.

Step 7 Enter a name in the partition name field and provide a description; otherwise, use the default partition name and description.

Step 8 Click the **Next** button.

The Manager Calling Search Space window displays.

Step 9 Enter a name in the calling search space name field and provide a description; otherwise, use the default calling search space name and description.

The Available Partitions and Selected Partitions boxes under the Route Partitions for this Calling Search Space automatically list Partitions for the Manager Calling Search Space. If the defaults that are provided are not wanted, the administrator can choose the applicable partition from the Available Partitions box. Use the up and down arrows to move partitions from one box to the other.

Step 10 Click the **Next** button.

The IPMA Calling Search Space window displays.

Step 11 Enter a name in the calling search space name field and provide a description; otherwise, use the default calling search space name and description.

The Available Partitions and Selected Partitions boxes under the Additional Route Partitions for This Calling Search Space automatically list Partitions for the IPMA Calling Search Space. If the defaults that are provided are not wanted, the administrator can choose the applicable partition from the Available Partitions box. Use the up and down arrows to move partitions from one box to the other.

Step 12 Click the **Next** button.

If you have existing calling search spaces that are configured in the system, the Existing Calling Search Spaces window displays; otherwise, the Existing Calling Search Spaces window does not display (proceed to Step 13).

Cisco IPMA requires that existing calling search spaces add the prefix Generated_IPMA and Generated_IPMA_Everyone partitions. The Available and Selected Partitions boxes under the Calling Search Spaces Configured with IPMA Partitions automatically list these partitions. Use the up and down arrows to move partitions from one box to the other.

Note The prefix that is added to the existing calling search spaces may change if the administrator has changed the names of the partitions in Steps 5 and 7.

Step 13 Click the **Next** button.

The IPMA CTI Route Point window displays.

Step 14 Enter a name in the CTI route point name field; otherwise, use the default CTI route point name.

Step 15 From the drop-down selection list box, choose the appropriate device pool.

Step 16 Enter a route point directory number; otherwise, use the default route point directory number.

Step 17 Click the **Next** button.

The IPMA Phone Service window displays.

Step 18 Enter the IPMA Phone Service name; otherwise, use the default IPMA Phone Service name.

Step 19 From the drop-down selection list box, choose the primary IPMA server or enter a server name or IP address in the Enter Server Name/IP Address field.

Step 20 Click the **Next** button.

The Cisco IPMA Configuration Wizard Confirmation window displays. It provides all the information that the administrator chose while using the configuration wizard. If the information is not correct, the administrator can cancel the configuration process or return to the previous configuration windows.

Step 21 To allow the configuration process to execute, click the **Finish** button; otherwise, to cancel the configuration process, click the **Cancel** button.

Upon completion, a final status window displays. The window shows the success or failure of each part of the wizard.

Any errors that the configuration wizard generates get sent to the trace file that is located in /var/log/active/tomcat/logs/ccmadmin/log4j/ccmadmin*.log.

This file can be accessed by using the following CLI command:

```
file get activelog tomcat/logs/ccmadmin/log4j
```

With the data that is collected from the configuration windows, the wizard automatically creates the partitions, calling search spaces, a route point, and the IPMA phone service. The wizard populates the Cisco IP Manager Assistant service parameters in the IPMA Device Configuration Defaults section of the Service Parameters Configuration window. Additionally, the wizard creates the IPMA manager phone template, the IPMA assistant phone template, and the Everyone phone template that BAT uses to configure phones for use with Cisco IPMA. Refer to the *Cisco CallManager Bulk Administration Guide* for information about configuring the manager and assistant devices.

Calling Search Space and Partitions

A Cisco IPMA route point intercepts calls for the managers and determines where to route them; therefore, all calls for the managers should flow through the route point first.

To accomplish the call flow, Cisco IPMA uses calling search spaces. Calls from lines that the Cisco IPMA service must route or act upon should have a calling search space that has the route point partition (you can call this partition IPMA) that is configured as the primary partition, and you can call the secondary partition the Everyone partition. See the following example.

Note For a manager who has multiple lines and who uses proxy line support, those lines must fall in the range covered by the route point (for example, a route point of 1xxx means that manager lines must fall in 1000 - 1999 range).

Example

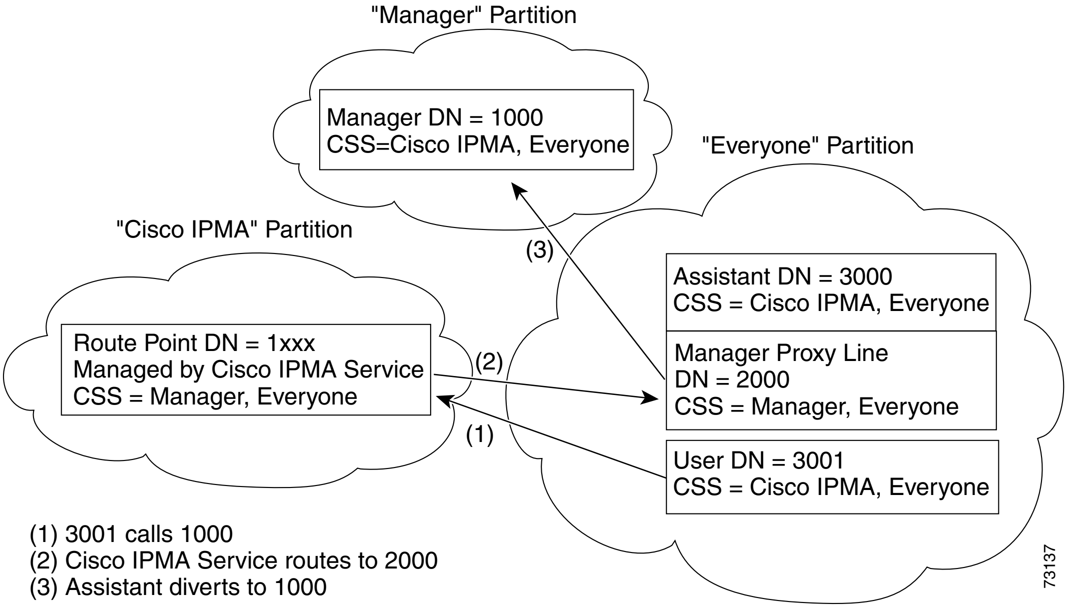
A user (in Everyone partition) places a call to a manager primary line (in Manager partition). Because the partition for the originating call does not include the manager primary line, the manager line number gets searched through the calling search space. The order of priority of the partitions in the calling search space provides basis for the search. Because the user line has a calling search space that comprises IPMA and Everyone, the search for the manager primary line begins with the IPMA partition. Because the Cisco IPMA route point matches the manager primary number, the call gets presented to the route point. The Cisco IPMA service that is monitoring the route point gets the call and routes the call by using the manager settings.

All lines that have calls that should go through a route point should have a calling search space that is called IPMA and Everyone. Examples of lines that require this calling search space configuration include manager primary and private lines, assistant primary line, and all other user lines.

All lines that have calls that should go directly to the manager without having the routing logic applied on them should have a calling search space that is called Managers and Everyone. Examples of lines that require this calling search space configuration include Cisco IPMA route point and assistant proxy lines.

See Figure 2-4 for an example of the calling search space and partition configuration.

Figure 2-4 Cisco IPMA Calling Search Space and Partition Configuration Example for Proxy Line Support



Configuration Tips

- Create three partitions that are called Cisco IPMA, Manager, and Everyone.
- Create a calling search space that is called CSS-M-E, which contains the partitions Manager and Everyone.
- Create a calling search space that is called CSS-I-E, which contains the partitions Cisco IPMA and Everyone
- Configure the manager primary and private directory numbers (DN) in the partition that is called Manager.
- Configure all assistants lines and other users lines in the partition that is called Everyone.
- Configure the Cisco IPMA route point in the partition that is called Cisco IPMA.

Cisco IPMA Route Point

You can have only one Cisco IPMA route point for each server. The directory numbers of Cisco IPMA route points must match the primary and private directory numbers of the manager; otherwise, the Cisco IPMA service routes calls inappropriately. Cisco recommends the use of wild cards to satisfy this condition.

Configuration Tips

- Create a route point that is called IPMA_RP.
- Configure the directory numbers of the route point to match the primary and private directory numbers of the managers (for example, for managers whose primary directory numbers are 1000-1999, create a route point DN as 1xxx for line 1; for managers whose primary directory numbers are 2000-2999, create a route point DN as 2xxx for line 2). Configure the directory numbers in the Cisco IPMA partition with a calling search space of CSS-M-E.

- Configure Call Forward No Answer with Destination Internal/External as Route Point DN (for example, CFNA as 1xxx for the Route Point DN 1xxx) with a calling search space of CSS-M-E. Call Forward No Answer forwards the call to the manager if the IPMA service is not available.

Setting the Service Parameters for Cisco IPMA

Service Parameters for the Cisco IPMA service comprise two categories: general and clusterwide. Specify clusterwide parameters once for all Cisco IPMA services. Specify general parameters for each Cisco IPMA service that is installed.

Set the Cisco IPMA service parameters by using Cisco CallManager Administration to access the service parameters (**System > Service Parameters**). Choose the server where the Cisco IPMA application resides and then choose the Cisco IP Manager Assistant service.

Cisco IPMA includes the following service parameters that must be configured:

- Clusterwide
  - Cisco IPMA Server (Primary) IP Address—No default. Administrator must manually enter this IP address.
  - Cisco IPMA Server (Backup) IP Address—No default. Administrator must manually enter this IP address.
  - Cisco IPMA Server Port—Default specifies Port 2912.
  - Cisco IPMA Assistant Console Heartbeat Interval—Default specifies 30 seconds. This interval timer specifies how long it takes for the failover to occur on the assistant console.
  - Cisco IPMA Assistant Console Request Timeout—Default specifies 30 seconds.
  - Cisco IPMA RNA Forward Calls—Default specifies False. If the parameter is set to True, an assistant phone that does not get answered will forward to another assistant phone.
  - Cisco IPMA RNA Timeout—Default specifies 10 seconds. RNA timeout specifies how long an assistant phone can go unanswered before the call is forwarded to another assistant phone. If Call Forward No Answer (CFNA) and RNA timeout are both configured, the first timeout occurrence takes precedence.
  - CTIManager Connection Security Flag—This service parameter indicates whether security for Cisco IPMA service CTIManager connection is enabled or disabled. If enabled, Cisco IPMA will open a secure connection to CTIManager by using the Application CAPF profile that is configured in the CAPF Profile Instance Id for Secure Connection to CTIManager service parameter.
- Cisco IPMA Service Parameters for each server
  - CTIManager (Primary) IP Address—No default. Enter the IP address of the primary CTIManager that will be used for call control.
  - CTIManager (Backup) IP Address—No default. Administrator must manually enter this IP address.
  - Route Point Device Name for Proxy Mode—No default. Choose the Cisco IPMA route point device name (that you configure by using **Device > CTI Route Point**).
  - CAPF Profile Instance Id for Secure Connection to CTIManager—This service parameter specifies the Instance Id of the Application CAPF Profile for the Application User IPMASecureSysUser that this Cisco IPMA server will use to open a secure connection to CTIManager. You must configure this parameter if CTIManager Connection Security Flag is enabled.

Cisco IPMA includes the following clusterwide parameters that must be configured if you want to use the IPMA automatic configuration for managers and assistants:

- Softkey Templates
  - Assistant Softkey Template—Default specifies Standard IPMA Assistant softkey template. This parameter specifies the softkey template that is assigned to the assistant device during IPMA assistant automatic configuration.
  - Manager Softkey Template for Proxy Mode—Default specifies Standard IPMA Manager softkey template. This parameter specifies the softkey template that is assigned to the manager device during IPMA manager automatic configuration.
  - Manager Softkey Template for Shared Mode—Default specifies Standard IPMA Shared Mode Manager. This service parameter does not apply to proxy line support.
- IPMA Device Configuration Defaults
  - Manager Partition—No default. This parameter specifies the partition that the IPMA automatic configuration assigns to the manager line(s) that IPMA handles on the manager device. Enter a partition that exists in the system. If you run the Cisco IPMA Configuration Wizard, the wizard populates this value.
  - All User Partition—No default. This parameter specifies the partition that the IPMA automatic configuration assigns to the proxy line(s) and the intercom line on the assistant device as well as the intercom line on the manager device. Enter a partition that exists in the system. If you run the Cisco IPMA Configuration Wizard, the wizard populates this value.
  - IPMA Calling Search Space—No default. This parameter specifies the calling search space that the IPMA automatic configuration assigns to the manager line(s) that IPMA handles and the intercom line on manager device as well as the assistant intercom line on assistant device. Enter a calling search space that exists in the system. If you run the Cisco IPMA Configuration Wizard, the wizard populates this value.
  - Manager Calling Search Space—No default. This parameter specifies the calling search space that the IPMA automatic configuration assigns to the proxy line(s) on the assistant device. Enter a calling search space that exists in the system. If you run the Cisco IPMA Configuration Wizard, the wizard populates this value.
  - Cisco IPMA Phone Service—No default. This parameter specifies the IPMA phone service that the automatic configuration assigns to the manager device. If you run the Cisco IPMA Configuration Wizard, the wizard populates this value.
- Proxy Directory Number Range
  - Starting Directory Number—No default. The Starting Directory Number and the Ending Directory Number parameters provide a range of proxy numbers that are available for the IPMA assistant configuration. The Starting Directory Number parameter specifies the first directory number in the range. The next available number in the range displays in the Proxy Line field in the User Configuration window when you are configuring an assistant.
  - Ending Directory Number—No default. The Starting Directory Number and the Ending Directory Number parameters provide a range of proxy numbers that are available for the IPMA assistant configuration. The Ending Directory Number parameter specifies the last directory number in the range. If you enter a smaller value in the Ending Directory Number field than you do in the Starting Directory Number field, an error displays when you access the IPMA configuration of an assistant in the User Configuration window.

- Proxy Directory Number Prefix
  - Number of Characters to be Stripped from Manager Directory Number—Default specifies 0. This parameter specifies the number of characters that Cisco CallManager strips from a manager IPMA directory number (DN) in the process of generating a proxy DN. You can use this parameter along with the Prefix for Manager Directory Number parameter to generate a proxy DN. For example, if you strip 2 digits from a manager DN of 2002 and add a prefix of 30 (specified in the Prefix for Manager Directory Number service parameter), Cisco CallManager generates a proxy DN of 3002. You can strip 0 to 24 characters.
  - Prefix for Manager DN—No default. This parameter specifies the prefix that Cisco CallManager adds to a manager DN in the process of generating the proxy DN. For example, if manager DN is 1001, number of characters to be stripped is 0, and the prefix is *, Cisco CallManager generates a proxy DN of *1001. The maximum prefix length equals 24.

Security Considerations

Cisco IPMA supports a secure connection to CTI (transport layer security connection).

The administrator must configure a CAPF profile (one for each IPMA node) by choosing **User Management > Application User CAPF Profile**. From the Application User drop-down list box that is on the Application User CAPF Profile Configuration window, the administrator chooses IPMASecureSysUser.

For more information about configuring security for IPMA, see the information on the CTIManager Connection Security Flag and the CAPF Profile Instance Id for Secure Connection to CTIManager service parameters in the "Setting the Service Parameters for Cisco IPMA" section on page 2-18.

The *Cisco CallManager Security Guide* provides detailed security configuration procedures for CTI applications.

Starting the Cisco IPMA Service

Cisco IPMA service runs as an application on Cisco Tomcat. To start or stop the Cisco IPMA service, use the Serviceability Control Center Feature Services window.

Cisco IP Phone Service Configuration

Add the Cisco IPMA service as a new Cisco IP Phone Service. Configure a name, description, and the URL for the Cisco IPMA service. The name and description that you enter should be in the local language because it displays on the manager Cisco IP Phone. For more information, see Cisco IP Phone Services Configuration in the *Cisco CallManager Administration Guide*.

Provide a URL by using the format
http://<server-ipaddress>:8080/ma/servlet/MAService?cmd=doPhoneService&Name=#DEVICENAME#

For example
http://123.45.67.89:8080/ma/servlet/MAService?cmd=doPhoneService&Name=#DEVICENAME#

Configuration Tips

To provide redundancy for the Cisco IP Phone Service, create a Cisco IP Phone Service that uses the host name rather than the IP address. The host name in DNS should resolve to both IPMA primary and backup IP addresses. The phone functionality for softkeys and filtering, as well as the phone service, will fail over automatically in the case of a failover.

Manager and Assistant Phone Configuration

You must configure devices for each IPMA manager and assistant. Before you begin, complete the following tasks, depending on the phone type.

Cisco IP Phone Model 7940/41, Model 7960/61, and Model 7970/71S

- Add a Cisco IP Phone model 7940/41, model 7960/61, or model 7970/71 for each manager and assistant that will be using Cisco IPMA. To add these phones, use one of the following methods:
  - Manually (**Device > Phone**)
  - Auto registration
  - BAT
- Assign the Standard IPMA Assistant phone button template for each assistant.

Cisco IP Phone Model 7940/41

You can use the Cisco IP Phone model 7940/41 for IPMA, but certain restrictions apply.

- Add a Cisco IP Phone model 7940/41 for each manager with the following items configured:
  - Two lines, one for the primary line and one for the intercom
  - Softkey template for manager with shared line support
- Add a Cisco IP Phone model 7940/41 for each assistant with the following items configured:
  - Two lines, one for the primary line and one for the intercom
  - Softkey template for assistant

Note Cisco supports the Cisco IP Phone model 7940/41 for IPMA but recommends the Cisco IP Phone model 7960/61 or model 7970/71 because they provide more functionality.

After you complete these tasks, configure the phones as described in the following sections:

- Manager Phones, page 2-22
- Assistant Phones, page 2-23
- Nonmanager and Nonassistant Phones, page 2-24

Manager Phones

The following section describes the IPMA requirements and tips for configuring a manager phone.

Manager Phone Configuration

Configure the manager Cisco IP Phones with the following settings:

- Standard IPMA Manager softkey template (must include the Immediate Divert and Transfer to Voice Mail softkeys)
- Primary line
- Additional lines if required
- Voice-messaging profile on primary line
- Incoming intercom line to support the auto answer with speakerphone or headset option
- Speed dial for outgoing intercom targets
- Subscribe to Cisco IP Phone Service, Cisco IPMA
- Set user locale

You can automate some of these settings by choosing the Automatic Configuration check box on the Cisco IPMA Manager Configuration window when you configure the manager. Automatic Configuration sets the following items for the manager device or device profile:

- Softkey template
- Subscription to IPMA phone service
- Calling search space and partition for IPMA-controlled selected lines and intercom line
- Auto answer with speakerphone for intercom line

Before you can automatically configure a manager phone, you must set the Cisco IPMA service parameters in the IPMA Device Configuration Defaults section. These parameters specify information such as which partition and calling search space to use for a manager line. You can enter these parameters manually, or you can populate the parameters by using the Cisco IPMA Configuration Wizard. For more information about these parameters, see the "Setting the Service Parameters for Cisco IPMA" section on page 2-18. For more information on the Cisco IPMA Configuration Wizard, see the "Cisco IPMA Configuration Wizard" section on page 2-13.

After you enter the appropriate service parameters, you can automatically configure a manager phone by choosing the **Automatic Configuration** check box on the Cisco IPMA Manager Configuration window and clicking **Save**. For step-by-step instructions, see the "Configuring a Manager and Assigning an Assistant for Proxy Line Mode" section on page 2-25.

Configuration Tips for Manager

- Do not configure Call Forward All Calls on the manager primary DN because the manager cannot intercept calls that are routed to the assistant proxy DN when Call Forward All Calls is set.
- Configure primary lines (IPMA-controlled lines) and assign DNs; use the Managers partition and the CSS-I-E calling search space for these lines if not using the automatic configuration.
- Configure an incoming intercom line and assign a DN; use the Everyone partition and the CSS-I-E calling search space if not using the automatic configuration.

IPMA supports the Cisco IP Phone model 7940. For more information, see the "Cisco IP Phone Model 7940/41" section on page 2-21.

Assistant Phones

The following section describes the IPMA requirements for configuring an assistant phone and provides tips on configuring an assistant phone.

Assistant Phone Configuration

Configure the assistant Cisco IP Phones with the following settings:

- Standard IPMA Assistant softkey template (must include the Immediate Divert and Transfer to Voice Mail softkeys)
- Default 14-button expansion module (optional for Model 7960 only)
- Standard IPMA Assistant phone button template (if using the 14-button expansion module)
- Primary line
- Proxy lines for each configured manager with a voice-mail profile that is the same as the manager voice-mail profile
- Incoming intercom line to support the auto answer with speakerphone or headset option
- Speed dial to incoming intercom line for each configured manager
- Set user locale

You can automate some of these settings by choosing the Automatic Configuration check box on the Cisco IPMA Assistant Configuration window when you configure the assistant. Automatic Configuration sets the following items for the assistant device or device profile:

- Softkey template
- Phone button template
- Calling search space and partition for existing proxy lines and intercom line
- Auto answer with speakerphone for intercom line
- Autogenerated proxy lines creation, if chosen

Before you can automatically configure an assistant phone, you must set the Cisco IPMA service parameters in the Device Configuration Defaults section. These parameters specify information such as which partition and calling search space to use for assistant proxy and intercom lines. You can enter these parameters manually, or you can populate the parameters by using the Cisco IPMA Configuration Wizard. For more information about these parameters, see the "Setting the Service Parameters for Cisco IPMA" section on page 2-18. For more information on the Cisco IPMA Configuration Wizard, see the "Cisco IPMA Configuration Wizard" section on page 2-13.

After you have entered the appropriate service parameters, you can automatically configure an assistant phone by choosing the **Automatic Configuration** check box on the Cisco IPMA Assistant Configuration window. For step-by-step instructions, see the "Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant" section on page 2-28.

Automatic configuration allows you to create a proxy line automatically (with the required calling search space and partition information) on the assistant phone. The autogenerated proxy numbers get generated from the values that you enter for the Proxy Directory Number Range and Proxy Directory Number Prefix service parameters as described in the "Setting the Service Parameters for Cisco IPMA" section on page 2-18.

Autogenerated numbers appear along with lines on the assistant device in the Proxy Line drop-down list box on the Cisco IPMA Assistant Configuration window when you configure the assistant. "Line" appears before existing lines on the assistant phone. "Auto" appears before each autogenerated number until the system adds that proxy line to an assistant phone. The system sets the calling search space and partition for the proxy line and the intercom line, if any, on the basis of the Cisco IPMA service parameter settings. For step-by-step instructions, see the "Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant" section on page 2-28.

Configuration Tips for Assistant

- Configure an incoming intercom line and assign a DN; use the Everyone partition and the CSS-I-E calling search space if you are not using the automatic configuration.
- Configure a proxy line and assign a DN for each manager that the assistant will support; use the Everyone partition and the CSS-M-E calling search space if you are not using the automatic configuration.

IPMA supports the Cisco IP Phone model 7940. For more information, see the "Cisco IP Phone Model 7940/41" section on page 2-21.

Nonmanager and Nonassistant Phones

In addition to configuring manager and assistant devices, configure all other users in the Cisco CallManager cluster. Proper configuration allows managers and assistants to make calls to and receive calls from all other users in the cluster.

Configuration Tips for Nonmanager and Nonassistant

- Use the Everyone partition for all other users.
- Use the CSS-I-E calling search space for all other users.
- If you use auto registration, perform the following tasks:
  - On the Device Pool Configuration window (**System > Device Pool**), choose CSS-I-E from the Calling Search Space for Auto-registration field.
  - On the Cisco CallManager Configuration window (**System > Cisco CallManager**), choose Everyone from the Partition field.
- If you use BAT, you can use the Everyone template that the Cisco IPMA Configuration Wizard created to add phones in the Everyone partition and the CSS-I-E calling search space.

Manager and Assistant Configuration

From the Cisco CallManager End User Configuration window, configure the settings for the managers and assistants who use the Cisco IPMA feature. You can configure IPMA in proxy line or shared line mode. To configure the manager and assistant for proxy line mode, see the "Configuring a Manager and Assigning an Assistant for Proxy Line Mode" section on page 2-25. To configure the manager and assistant for shared line mode, see the "Configuring a Manager and Assigning an Assistant for Shared Line Mode" section on page 3-16.

From the End User Configuration window, perform the following functions:

- Choose manager and assistant devices
- Automatically configure a manager or assistant device, if you want one
- Choose the local language in which the User Information window displays.

- Choose the Cisco IPMA Manager or Cisco IPMA Assistant configuration window to configure the following IPMA settings:
  - Set up primary and incoming intercom lines for intercom capability. For example, configure extension 3102 as the intercom line for the manager. This line will receive intercom calls from the assistant; for example, the assistant line 1 (1102) and line 2 (1103) display on the assistant console, and the assistant answers them.
  - Configure assistants for managers.
  - Set up proxy lines for each manager on the assistant phone. For example, assistant lines 4 and 5 take calls from manager lines 1102 and 1103.

The following sections provide details about configuring the manager and assistant settings:

- Configuring a Manager and Assigning an Assistant for Proxy Line Mode, page 2-25
- Deleting Cisco IPMA Information from the Manager, page 2-26
- Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant, page 2-28
- Deleting the Cisco IPMA Information from the Assistant, page 2-29

Configuring a Manager and Assigning an Assistant for Proxy Line Mode

Perform the following procedure to configure a Cisco IPMA manager and assign an assistant to the manager. To configure a new user, see "Adding an End User" in the *Cisco CallManager Administration Guide*.

Tip Configure Cisco IPMA manager information before configuring Cisco IPMA information for an assistant.

Procedure

Step 1 To configure the IPMA manager and to assign an assistant to an existing user, choose **User Management > End User**.

Step 2 To find the user that will be the IPMA manager, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

Step 3 To display user information for the chosen manager, click the user name.

The End User Configuration window displays.

Step 4 To configure IPMA information for the manager, choose the **Cisco IPMA Manager** from the Related Links drop-down list box and click Go.

Step 5 The Cisco IPMA Manager Configuration window displays and contains manager information, assistant information, and IPMA-controlled lines for the chosen user.

Tip To view existing assistant configuration information, click the assistant name in the Associated Assistants list and click the **Edit Assistant** link. The Cisco IPMA Assistant IPMA Configuration information displays. To return to the manager configuration information, click the manager name in the Associated Managers list on the Cisco IPMA Assistant Configuration window.

Step 6 To associate a device name or device profile with a manager, choose the device name or device profile from the Device Name/Profile selection box. Extension Mobility can optionally use device profiles. For information about using Cisco CallManager Extension Mobility with Cisco IPMA, see the "Extension Mobility" section on page 2-7.

Note If the manager telecommutes, click the Mobile Manager check box and optionally choose Device Profile. When Device Profile is chosen, the manager must log on to the phone by using extension mobility before accessing IPMA.

Step 7 From the Intercom Line selection box, choose the intercom line appearance for the manager, if applicable.

Step 8 To assign an assistant to the manager, choose an assistant from the Available Assistants list and click the down arrow to move the chosen assistant to the Associated Assistants list.

Step 9 From the Available Lines selection box, choose a line that you want Cisco IPMA to control, and click the down arrow to make the line display in the Selected Lines selection box. Configure up to five IPMA-controlled lines.

To remove a line from the Selected Lines selection box and from Cisco IPMA control, click the up arrow.

Step 10 To automatically configure the softkey template, subscription to the IPMA phone service, calling search space and partition for IPMA-controlled selected lines and intercom line, and auto answer with speakerphone for intercom line for the manager phone based on the IPMA service parameters, check the **Automatic Configuration** check box.

Step 11 Click the **Save** button.

The update takes effect immediately.

If you checked the Automatic Configuration check box and the service parameters are invalid, a message displays.

Upon successful completion of the automatic configuration, the manager device resets. If you configured a device profile, the manager must log out and log in to the device for settings to take effect.

Note When non-IPMA changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco IPMA and log in before the changes occur.

Additional Information

See the "Related Topics" section on page 2-33.

Deleting Cisco IPMA Information from the Manager

Perform the following procedure to delete Cisco IPMA information for a manager. To delete non-IPMA information for a manager, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Procedure

Step 1 To search for the manager for whom you want to delete IPMA information, choose **User Management > End User** from Cisco CallManager Administration.

Step 2 From the Find and List Users window, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

A list of configured users displays.

Step 3 Choose the manager whose Cisco IPMA information you want to delete.

Step 4 From the Related Links drop-down list box, click **Cisco IPMA Manager**.

The Cisco IPMA Manager Configuration window displays and contains IPMA manager configuration information.

Step 5 Click the **Delete** button.

The update takes effect immediately.

Additional Information

See the "Related Topics" section on page 2-33.

Updating the Manager Cisco IPMA Configuration

Perform the following procedure to update Cisco IPMA information for a manager. To update non-IPMA information for a manager, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Procedure

Step 1 To search for the manager for whom you want to update IPMA information, choose **User Management > End User** from Cisco CallManager Administration.

Step 2 From the Find and List Users window, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

A list of configured users displays.

Step 3 Choose the manager whose Cisco IPMA information you want to update.

Step 4 From the Related Links drop-down list box, click **Cisco IPMA Manager**.

The Cisco IPMA Manager Configuration window displays and contains IPMA manager configuration information.

Step 5 Update the information that you want changed such as device name, IPMA-controlled lines, or intercom line appearance.

Note The system automatically configures the softkey template, subscription to the IPMA phone service, calling search space and partition for IPMA-controlled selected lines and intercom line, and auto answer with speakerphone for intercom line for the manager phone based on the IPMA service parameters when the **Automatic Configuration** check box is checked.

Step 6 Click the **Save** button.

The update takes effect immediately.

Note When non-IPMA changes such as name, user locale, or PIN are made to a user, the user (manager or assistant) must log out of Cisco IPMA and log in for the changes to occur.

Additional Information

See the "Related Topics" section on page 2-33.

Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant

Use the Cisco IPMA Assistant Configuration of the End User Configuration window to configure the following items:

- Device name of the assistant phone
- Intercom line that the assistant uses to answer the manager calls (optional)
- Primary line to make outgoing calls (optional)
- Proxy line of the assistant phone that is associated with the manager, the manager name, and the manager line. For example, the assistant phone line 3 gets used to answer manager Mary Smith phone line 2.

A proxy line specifies a phone line that appears on the assistant Cisco IP Phone. Cisco IPMA uses proxy lines to manage calls that are intended for a manager; for example, manager1. If the call-routing software determines that the call should be presented to the assistant because manager1 cannot accept the call, the call routes to the proxy line that is configured for manager1 on the assistant Cisco IP Phone.

You can manually configure a line on the assistant phone to serve as the proxy line, or you can use automatic configuration to generate a DN and to add the line to the assistant phone.

For information about configuring shared and intercom lines for Cisco IPMA with shared line mode, see the "Configuring Shared and Incoming Intercom Lines for the Assistant" section on page 3-18.

When you display IPMA information for the assistant, the system generates DNs on the basis of IPMA service parameter entries in the Proxy Directory Number Range and Proxy Directory Prefix sections. For more information about these service parameters, see the "Setting the Service Parameters for Cisco IPMA" section on page 2-18.

Perform the following procedure to configure the proxy and incoming intercom line appearances for an assistant. To configure a new user, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Tip Before configuring the Cisco IPMA information for an assistant, you must configure the Cisco IPMA manager information and assign an assistant to the manager. See "Configuring a Manager and Assigning an Assistant for Proxy Line Mode" section on page 2-25.

Before You Begin

If you want to automatically configure the proxy line on the assistant phone, configure the IPMA service parameters in the Proxy Directory Number Range and Proxy Directory Number Prefix sections.

Procedure

Step 1 To configure IPMA for an assistant and assign proxy and incoming intercom lines, choose **User Management > End User**.

Step 2 To find the user that will be the IPMA assistant, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

Step 3 To display user information for the chosen assistant, click the user name.

The End User Configuration window displays.

Step 4 To configure IPMA information for the assistant, choose **Cisco IPMA Assistant** from the Related Links drop-down list box and click Go.

The Cisco IPMA Assistant Configuration window displays.

Step 5 From the Device Name selection box, choose the device name to associate with the assistant.

Step 6 From the Intercom Line Appearance selection box, choose the incoming intercom line appearance for the assistant.

Step 7 Use the selection boxes in the Manager Association to Assistant Line area to assign and associate manager line numbers to the assistant line numbers.

Step 8 In the Available Lines selection box, choose the assistant line. The word "Auto" precedes the autogenerated proxy lines. If you want Cisco CallManager to create an autogenerated proxy line on the assistant phone, choose an autogenerated proxy line and ensure that the **Automatic Configuration** check box is checked.

Note The system automatically sets the softkey template as well as the calling search space and partition for existing proxy lines and intercom line on the basis of the Cisco IPMA service parameter settings when the Automatic Configuration check box is checked. Additionally, the system sets auto answer with speakerphone for intercom line.

Step 9 In the Manager Name selection box, choose the manager for whom this proxy line will apply.

Step 10 In the Manager Line selection box, choose the manager line for which this proxy line will apply.

Step 11 Click the **Save** button.

The update takes effect immediately. If you chose automatic configuration, the assistant device automatically resets.

Additional Information

See the "Related Topics" section on page 2-33.

Deleting the Cisco IPMA Information from the Assistant

Perform the following procedure to delete Cisco IPMA information for an assistant. To delete non-IPMA information for an assistant, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Procedure

Step 1 To search for the assistant for whom you want to delete IPMA information, choose **User Management > End User** from Cisco CallManager Administration.

Step 2 From the Find and List Users window, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

A list of configured users displays.

Step 3 Choose the assistant whose Cisco IPMA information you want to delete.

Step 4 From the Related Links drop-down list box, click **Cisco IPMA Assistant**.

The Cisco IPMA Assistant Configuration window displays and contains IPMA assistant configuration information.

Step 5 Click the **Delete** button.

The update takes effect immediately.

Note When non-IPMA changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco IPMA and log in before the changes occur.

Additional Information

See the "Related Topics" section on page 2-33.

Updating the Assistant Cisco IPMA Configuration

Perform the following procedure to update Cisco IPMA information for an assistant. To update non-IPMA information for an assistant, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Procedure

Step 1 To search for the assistant for whom you want to update IPMA information, choose **User Management > End User** from Cisco CallManager Administration.

Step 2 From the Find and List Users window, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

A list of configured users displays.

Step 3 Choose the assistant whose Cisco IPMA information you want to update.

Step 4 From the Related Links drop-down list box, click **Cisco IPMA Assistant**.

The Cisco IPMA Assistant Configuration window displays and contains IPMA assistant configuration information.

Step 5 Update the information such as device name, intercom line, or manager association information that you want changed.

Note The system automatically configures the softkey template, subscription to the IPMA phone service, calling search space and partition for IPMA-controlled selected lines and intercom line, and auto answer with speakerphone for intercom line for the manager phone based on the IPMA service parameters when the **Automatic Configuration** check box is checked.

Step 6 Click the **Save** button.

The update takes effect immediately.

Note When non-IPMA changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco IPMA and log in before the changes occur.

Additional Information

See the "Related Topics" section on page 2-33.

Dial Rules Configuration

The administrator uses dial rules configuration to add and sort the priority of dialing rules. Dial rules for Cisco IPMA automatically strip numbers from or add numbers to telephone numbers that the assistant dials from the directory search window in the Assistant Console. For example, a dial rule can automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

The following sections provide additional information on application dial rules:

- Application Dial Rules Configuration Design, *Cisco CallManager System Guide*
- Application Dial Rules Configuration Error Checking, *Cisco CallManager System Guide*

Providing Information to Cisco IPMA Managers and Assistants

Install the assistant console application for Cisco IPMA by accessing a URL. The administrator sends the URL, in the "Installing the Assistant Console Application" section on page 2-32, to the assistant.

Note The assistant console application installation program supports Netscape 7.1 or later and Microsoft Internet Explorer 6.0 or later.

Installing the Assistant Console Application

Note When upgrading from Cisco CallManager release 4.0 or 4.1 to release 5.0, you must reinstall the Assistant Console application.

Begin the installation by accessing the following URL:

https://<IPMA server>:8443/ma/Install/IPMAConsoleInstall.jsp

where

IPMA server specifies the IP address of the server that has the IPMA service running on it.

Tip You can localize the installer (with the proper localization pack) by including the proper parameter on the URL; for example, for French, you would include the following parameter at the end of the URL:?locale=fr_FR.

Assistant Console Dialog Options

The assistant console displays a dialog that contains the following options:

- Location to Install—The path of the directory where the assistant console software gets installed. The default specifies following path:

  c:\Program Files\Cisco\IPMA Assistant Console\
- Create Desktop Shortcut—Default specifies true. This parameter determines whether a shortcut is created on the assistant console.
- Create StartMenu Shortcut—Default specifies true. This parameter determines whether a shortcut is created in the Start menu (**Start > Programs > Cisco IPMA > IPMA Assistant Console**).
- Install JRE—Default specifies true. This parameter determines whether JRE is installed along with IPMA assistant console. If this option is turned off, the following configuration is required on the assistant console:
  - Install JRE 1.4.2_05 (international version) on the assistant console
  - Create an environment variable—IPMA_JRE on the assistant console, which gives the path to the JRE; for example, c:\Program Files\Jave\j2re1.4.2_05

Manager Configuration

Managers can customize their feature preferences from the Manager Configuration window by using the following URL:

https://<IPMA server>:8443/ma/desktop/maLogin.jsp

where

IPMA server specifies the IP address of the server that has the Cisco IPMA service running on it.

Note The Manager Configuration only supports Microsoft Internet Explorer 6.0 or later.

The administrator must send this URL to the manager.

Additional Information

See the "Related Topics" section on page 2-33.

Related Topics

- Softkey Templates, *Cisco CallManager System Guide*
- Cisco IP Manager Assistant With Shared Line Support
- Cisco IPMA Service, page 2-2
- Cisco IP Phone Interface, page 2-4
- Cisco IPMA Configuration Wizard, page 2-13
- Cisco IP Phone Service Configuration, page 2-20
- Nonmanager and Nonassistant Phones, page 2-24
- Configuring a Manager and Assigning an Assistant for Proxy Line Mode, page 2-25
- Deleting Cisco IPMA Information from the Manager, page 2-26
- Updating the Manager Cisco IPMA Configuration, page 2-27
- Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant, page 2-28
- Deleting the Cisco IPMA Information from the Assistant, page 2-29
- Adding an End User, *Cisco CallManager Administration Guide*
- Associating Devices to an End User, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Manager Assistant User Guide*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Bulk Administration Guide*
- *Cisco CallManager Security Guide*

Cisco IP Manager Assistant With Shared Line Support

The Cisco IP Manager Assistant (Cisco IPMA) feature enables managers and their assistants to work together more effectively. Cisco IPMA supports two modes of operation: proxy line support and shared line support. The Cisco IPMA service supports both proxy line and shared line support in a cluster.

The feature comprises enhancements to phone capabilities for the manager and the assistant console application that are primarily used by the assistant.

Cisco CallManager users comprise managers and assistants. An assistant user handles calls on behalf of a manager. Cisco IPMA comprises features for managers and features for assistants.

This chapter provides the following information about Cisco IPMA:

- Introducing Cisco IPMA, page 3-1
- System Requirements for Cisco IPMA with Shared Line Support, page 3-5
- Interactions and Restrictions, page 3-6
- Installing and Activating Cisco IPMA, page 3-8
- Configuring Cisco IPMA with Shared Line Support, page 3-9
- Providing Information to Cisco IPMA Managers and Assistants, page 3-22
- Related Topics, page 3-23

Introducing Cisco IPMA

The following sections provide information about the Cisco IPMA feature:

- Cisco IPMA Architecture Overview, page 3-2
- Cisco IPMA Database Access Architecture, page 3-4
- Manager Interfaces, page 3-4
- Assistant Interfaces, page 3-4
- Softkeys, page 3-4
- Manager Assistant Administration Interface, page 3-5

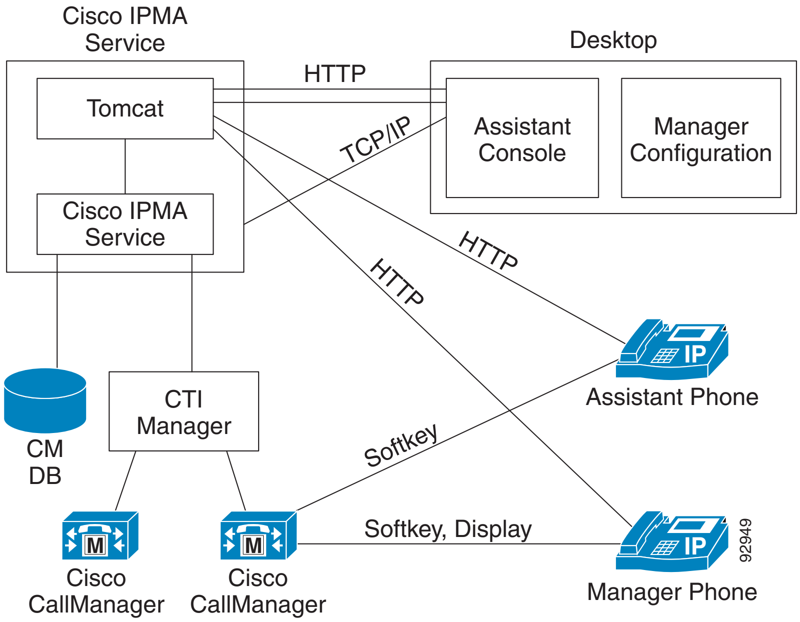
Cisco IPMA Architecture Overview

The Cisco IPMA feature architecture comprises the Cisco IPMA service, the assistant console application, and the Cisco IP Phone interfaces. See Figure 3-1.

Additional Information

See the "Related Topics" section on page 3-23.

Figure 3-1 Cisco IPMA Architecture



Cisco IPMA Service

Cisco Tomcat loads the Cisco IPMA service, a servlet. Cisco Tomcat gets installed at Cisco CallManager installation.

The Cisco IPMA service gets installed on all Cisco CallManager servers in a cluster. After installation, the administrator activates the service from Serviceability, which automatically starts IPMA. When started, the IPMA service checks to see whether it is one of the IPMA servers that is configured in the clusterwide service parameter, Cisco IPMA Server (Primary) IP Address. If it is, the IPMA service attempts to become the active Cisco IPMA service. Currently, a Cisco CallManager cluster supports only one active Cisco IPMA service.

The Cisco IPMA service performs the following tasks:

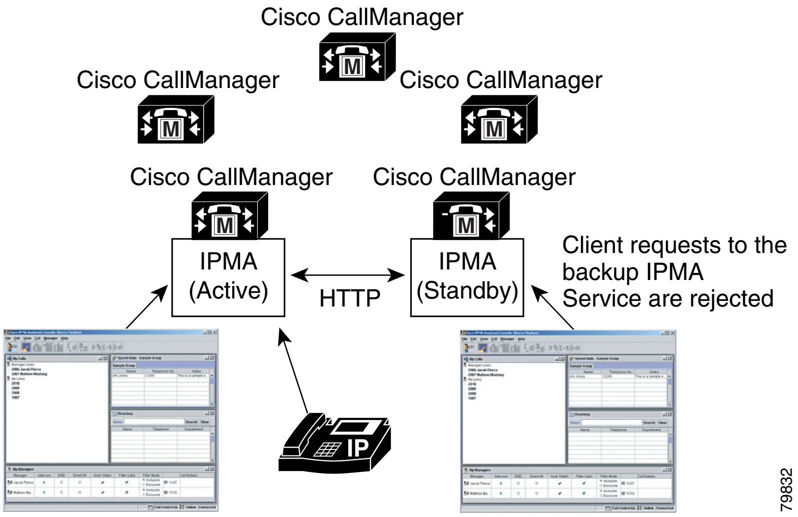
- Hosts the HTTP services that run on the manager phone.
- Hosts the web pages that the manager uses for configuration.
- Communicates to a Cisco CallManager cluster through the Cisco CTIManager for third-party call control. Cisco IPMA requires only one CTI connection for all users in a cluster.
- Accesses data from the database.
- Supports the Assistant Console application.

Cisco CallManager supports redundancy of the Cisco IPMA service. To achieve redundancy, you must configure a second Cisco IPMA service in the same cluster.

IPMA implements redundancy by using an active/standby server model. At any time, only one IPMA server remains active and servicing all assistant console applications and phones. The other server stays in a standby mode and will detect failures on the active server. When the backup server detects a failure, it takes over and becomes the active server. All connections that were active get restored on the new server, and service continues uninterrupted to the users.

If the active server fails, the Assistant Console application fails over automatically to the backup server. The Cisco IPMA Assistant Console Heartbeat Interval service parameter (see the "Setting the Service Parameters for Cisco IPMA" section on page 3-11) determines the time that the application takes to detect failure. A shorter heartbeat interval leads to faster failover. See Figure 3-2.

Figure 3-2 Cisco IPMA Redundancy



The Cisco IPMA service includes built-in security to help prevent unauthorized access to its services. The user ID and password that are collected at the assistant console get encrypted before they are sent over the network. The Assistant Console blocks nonauthorized users who are posing as assistants.

Assistant Console Interface

Cisco IPMA supports the following assistant console interfaces for managers and assistants:

- Assistant Console (used for call control, log on, assistant preferences, monitoring managers call activity, keyboard shortcuts)
- Manager configuration (used for configuring the immediate divert target)

Administrators use Cisco CallManager Administration, End User Configuration, to configure Cisco IPMA for managers and assistants. See "Manager Assistant Administration Interface" section on page 3-5.

Cisco CallManager makes the Cisco IPMA manager features Immediate Divert and Transfer to Voice Mail available through the Cisco IP Phone. Use a browser to access Manager configuration. Assistants use the Cisco IP Phone and the assistant console application. See "Manager Interfaces" section on page 3-4 and "Assistant Interfaces" section on page 3-4.

For more information about how to use the Cisco IPMA assistant console features, refer to the *Cisco IP Manager Assistant User Guide*.

Cisco IP Phone Interface

Assistants and managers use softkeys to access Cisco IPMA features. For more information about how to use the Cisco IPMA Phone features, refer to the *Cisco IP Manager Assistant User Guide*.

See "Manager Interfaces" section on page 3-4 and "Assistant Interfaces" section on page 3-4.

Cisco IPMA Database Access Architecture

The database stores all Cisco IPMA configuration information. When the manager or assistant logs in, the IPMA service retrieves all data that is related to the manager or assistant from the database and stores it in memory.

Manager Interfaces

The manager phone makes available the manager features with the exception of Manager Configuration. Cisco IPMA automatically logs a manager into the IPMA service when the Cisco IPMA service starts.

The manager accesses the Cisco IPMA features Do Not Disturb, Immediate Divert, and Transfer to Voice Mail from the Cisco IP Phone softkeys.

The state of the Do Not Disturb feature displays in the Status Window on the Cisco IP Phone.

Refer to the *Cisco IP Manager Assistant User Guide* for more information.

Assistant Interfaces

The assistant accesses the Cisco IPMA features by using the Assistant Console application and the Cisco IP Phone. The Assistant Console, an application, provides call-control functions such as answer, divert, transfer, and hold. The assistant uses the Assistant Console to log on and log off, to set up assistant preferences, and to display the manager configuration window that is used to configure manager preferences.

The Assistant Console displays the assistant lines and the manager shared lines. Assistants access the shared lines to manage calls that are intended for a manager.

You can access Intercom and Distinctive Ringing on the assistant Cisco IP Phone. When the assistant logs in from the Assistant Console, the soft keys Immediate Divert and Transfer to Voice Mail become active for the shared lines. Refer to the *Cisco IP Manager Assistant User Guide* for more information.

Softkeys

The Cisco IPMA feature supports softkeys such as Immediate Divert, Transfer to Voice Mail, and Do Not Disturb on the Cisco IP Phone. Softkeys only appear in their appropriate call state; for example, Transfer to Voice Mail does not appear if no active calls exist.

Cisco IPMA supports the following softkey templates:

- Standard IPMA Manager—Supports manager for proxy mode
- Standard IPMA Shared Mode Manager—Supports manager for shared mode
- Standard IPMA Assistant—Supports assistant in proxy or shared mode

Additionally, the system makes call-processing (such as hold and dial) softkeys available with the Standard User template. The administrator configures the appropriate softkey template for the devices that managers and assistants use.

Note The default process assigns call-processing softkey templates to devices.

Administrators can create custom softkey templates in addition to using the standard softkey templates that are included in Cisco CallManager. Use Softkey Template configuration in Cisco CallManager Administration to associate softkey templates with Cisco IPMA devices and to create custom softkey templates. See Softkey Template Configuration in the *Cisco CallManager Administration Guide*.

Manager Assistant Administration Interface

The administrator uses the User menu options of Cisco CallManager Administration to configure the manager and assistant. The administrator chooses the device for the manager and assistant and optionally chooses an incoming intercom line for the manager and assistant. The administrator sets up the shared line for the manager, which gets configured for the assistant.

See the "Manager and Assistant Configuration" section on page 3-15.

System Requirements for Cisco IPMA with Shared Line Support

Cisco IPMA with shared line support requires the following software components to operate:

- Cisco CallManager 5.0
- Microsoft Internet Explorer or Netscape Navigator:
  - Cisco IPMA administration (using Cisco CallManager Administration) supports Microsoft Internet Explorer (IE) 6.0 or later and Netscape 7.1 or later.
  - The Assistant Console application installation program supports Microsoft Internet Explorer (IE) 6.0 or later and Netscape 7.1 or later. (See the "Interactions and Restrictions" section on page 3-6 for more information.)
  - The Assistant Console application supports Microsoft Windows 2000 and Microsoft Windows XP.
  - The Manager Configuration application supports Microsoft Internet Explorer (IE) 6.0 or later.

The following SCCP phones support Cisco IPMA:

- Cisco IP Phone Model 7970/71
- Cisco IP Phone Model 7960/61
- Cisco IP Phone Model 7940/41 (See the "Restrictions" section on page 3-8.)

Note Cisco IP Phone Model 7960/61 and 7970/71 that is running Cisco IPMA may be equipped with a Cisco Model 7914 Expansion Module.

Because Cisco IPMA is installed automatically on the same server with Cisco CallManager, you do not require an additional server.

Interactions and Restrictions

The following sections describe the interactions and restrictions for Cisco IPMA:

- Interactions, page 3-6
- Restrictions, page 3-8

Interactions

The following sections describe how Cisco IPMA interacts with Cisco CallManager applications:

- Bulk Administration Tool, page 3-6
- Extension Mobility, page 3-6
- Reporting Tools, page 3-7
- Multilevel Precedence and Preemption (MLPP), page 3-8

Bulk Administration Tool

The administrator can use the Bulk Administration Tool (BAT) to add many users (managers and assistants) at once instead of adding users individually. Refer to the *Cisco CallManager Bulk Administration Guide* for more information.

Additional Information

See the "Related Topics" section on page 3-23.

Extension Mobility

A manager who uses the Cisco CallManager Extension Mobility feature can simultaneously use Cisco IPMA. The manager logs into the Cisco IP Phone by using Extension Mobility and then chooses the Cisco IPMA service. When the IPMA service starts, the manager can access assistants and IPMA features (such as Do Not Disturb).

To have access to Cisco CallManager Extension Mobility with IPMA, the administrator checks the Mobile Manager check box in the Cisco IPMA Manager Configuration window in Cisco CallManager Administration (accessed from the End user Configuration window). See the "Configuring a Manager and Assigning an Assistant for Shared Line Mode" section on page 3-16. For more information about configuring device profiles, see Configuring a New User Device Profile in the *Cisco CallManager Administration Guide*. For more information about Cisco CallManager Extension Mobility, see Chapter 1, "Cisco CallManager Extension Mobility."

Reporting Tools

Cisco IPMA provides statistical information in the CDR Analysis and Reporting (CAR) tool and provides a summary of changes to configurations in a change log. The following sections describe these reporting tools.

CDR Analysis and Reporting

Cisco IPMA supports call-completion statistics for managers and assistants and inventory reporting for managers and assistants. The CDR Analysis and Reporting (CAR) tool supports call-completion statistics. Cisco CallManager Serviceability supports inventory reporting. Refer to the *Cisco CallManager Serviceability System Guide,* the *Cisco CallManager Serviceability Administration Guide*, and the *CDR Analysis and Reporting Administration Guide* for more information.

IPMAChangeLog*.txt

The administrator can view a summary of changes that are made to the Manager or Assistant Configurations. A manager can change defaults by accessing the Manager Configuration from a URL.

An assistant can change the manager defaults from the Assistant Console.

Note Refer to the *Cisco IP Manager Assistant User Guide* for information about the URL and Manager Configuration.

When changes are made, the information gets sent to a log file that is called ipma_changeLogxxx.log. The log file resides on the server that runs the IPMA service at the following location:

file get activelog tomcat/logs/ipma/log4j/

The administrator can download this file from the server by using the Trace Collection Tool in the Serviceability Real-Time Monitoring Tool (RTMT). Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

The log file contains the following fields:

- LineNumber—The line in the log file with information about changes
- TimeStamp—The time that the configuration changed
- for Manager/Assistant—Designation of whether the change is for the manager or the assistant
- for Userid—The userid of the manager or assistant that is being changed
- by Manager/Assistant—Designation of whether the change was made by the manager or the assistant
- by Userid—The userid of the manager or assistant who made the change
- Parameter Name—What changed; for example, divert target number
- Old Value—The value of the information before the change
- New Value—The value of the information after the change

Because the information in the log file is comma delimited, the administrator can open the log file by using a spreadsheet application such as Microsoft Excel. Use the following procedure to save the log file contents to the Microsoft Excel application.

Procedure

Step 1 Start the Microsoft Excel application.

Step 2 Choose **File > Open** to open the IPMA.txt file.

Step 3 Choose the Original data type, file type as Delimited and click **Next**.

Step 4 Choose Delimiters as Comma and click **Next**.

Step 5 When complete, click **Finish**.

Multilevel Precedence and Preemption (MLPP)

The following points describe the interactions between Cisco IPMA with shared line support and MLPP:

- The system preserves call precedence in the handling of calls by IPMA. For example, when an assistant diverts a call, the system preserves the precedence of the call.
- Because IPMA does not have knowledge of the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.

Restrictions

The following restrictions apply to Cisco IPMA:

- Cisco IPMA does not support Cisco IP SIP Phones.
- One manager can have up to 10 assigned assistants.
- One assistant can support up to 33 managers (if each manager has one IPMA-controlled line).
- Cisco IPMA supports up to 1024 managers and 1024 assistants per Cisco CallManager cluster.
- Cisco IPMA Assistant Console does not support hunt groups/queues.
- Cisco IPMA Assistant Console does not support record and monitoring.
- Cisco IPMA Assistant Console does not support on hook transfer (the ability to transfer a call by pressing the Transfer softkey and going on hook to complete the transfer).
- Cisco IPMA Assistant Console does not support the one-touch Call Pickup feature.
- Cisco IP Phone Model 7940 supports only two lines or speed-dial buttons.
- To install the Assistant Console application on a computer with Microsoft IE version 6 on Windows XP, install the Microsoft Java Virtual Machine (JVM) with Windows XP Service Pack 1 before the Assistant Console installation.

Installing and Activating Cisco IPMA

Cisco Tomcat loads the Cisco IPMA, a servlet. Cisco Tomcat gets installed and started at Cisco CallManager installation. For more information, see the "Cisco IPMA Service" section on page 3-2.

The administrator performs the following three steps after installation to make Cisco IPMA available for system use:

1. Use Cisco CallManager Serviceability Service Activation, located on the Tools menu, to activate the Cisco IP Manager Assistant service. Refer to the *Cisco CallManager Serviceability Administration Guide*.
2. Configure the applicable service parameters for the Cisco IP Manager Assistant service. See the "Setting the Service Parameters for Cisco IPMA" section on page 3-11.
3. Use Serviceability Control Center Feature Service to stop and start the Cisco IPMA service. See the "Starting the Cisco IPMA Service" section on page 3-13.

Note If the managers and assistants will require Cisco IPMA features to display (on the phone and assistant console) in any language other than English, verify that the locale installer is installed before configuring Cisco IPMA. Refer to the Cisco IP Telephony Locale Installer documentation.

Configuring Cisco IPMA with Shared Line Support

For successful configuration of Cisco IPMA, review the steps in the configuration checklist, perform the user and device configuration requirements, and configure the managers and assistants.

Note Cisco IPMA with shared line support coexists in the same Cisco CallManager cluster with Cisco IPMA with proxy line support. For configuration information about proxy line support, see Cisco IP Manager Assistant With Proxy Line Support.

The following sections provide configuration information:

- Configuration Checklist for Cisco IPMA with Shared Line Support, page 3-9
- Setting the Service Parameters for Cisco IPMA, page 3-11
- Security Considerations, page 3-13
- Starting the Cisco IPMA Service, page 3-13
- Manager and Assistant Phone Configuration, page 3-13
- Manager and Assistant Configuration, page 3-15

Configuration Checklist for Cisco IPMA with Shared Line Support

Table 3-1 shows the logical steps for configuring the Cisco IP Manager Assistant with shared line support in Cisco CallManager.

Before You Begin

The information in the checklist assumes that you have already configured the phones and the users and have associated the devices to the users. Additionally, for shared line appearances between managers and assistants, you must configure the same directory number on the manager primary line and assistant secondary line. Refer to Adding an End User, Associating Devices to an End User, Configuring Cisco IP Phones, and Directory Number Configuration Overview in the *Cisco CallManager Administration Guide*.

Table 3-1 Cisco IP Manager Assistant Configuration Checklist with Shared Line Support

Configuration Steps		Related Procedures and Topics
Step 1	Using Cisco CallManager Serviceability, Service Activation, activate Cisco IP Manager Assistant service.	*Cisco CallManager Serviceability Administration Guide*
Step 2	Configure IPMA service parameters for shared line support.	Setting the Service Parameters for Cisco IPMA, page 3-11 Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 3	• Configure the application user CAPF profile (optional). • Configure IPMA service parameters for security (optional).	Setting the Service Parameters for Cisco IPMA, page 3-11 Security Considerations, page 3-13
Step 4	Using the Serviceability Control Center Feature Services, stop and start the Cisco IPMA service.	Starting the Cisco IPMA Service, page 3-13
Step 5	Add Cisco IP Phone model 7960 or 7970 phone button template.	Configuring Phone Button Templates, *Cisco CallManager Administration Guide*
Step 6	Configure manager and assistant Cisco IP Phone parameters: • Set up manager phone. • Set up assistant phone.	Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*
Step 7	Configure manager phone settings: • Assign the softkey template for shared line mode. • Add primary lines. (Use the same DN and partition for the assistant secondary line DN.) • Set up voice-mail profile on primary line. • Add incoming intercom line (optional). • Add speed dial for outgoing intercom targets (optional). • Set user locale. • Reset the phone. **Tip** To automatically configure some manager phone settings, choose the automatic configuration check box on the User Information window when configuring the manager. For more information, see the "Manager Phones" section on page 3-14.	Manager and Assistant Phone Configuration, page 3-13 Finding a Phone, *Cisco CallManager Administration Guide* Deleting a Phone, *Cisco CallManager Administration Guide* Directory Number Configuration Overview, *Cisco CallManager Administration Guide* Configuring Speed-Dial Buttons, *Cisco CallManager Administration Guide* Resetting a Phone, *Cisco CallManager Administration Guide*

Table 3-1 Cisco IP Manager Assistant Configuration Checklist with Shared Line Support (continued)

Configuration Steps		Related Procedures and Topics
Step 8	Configure assistant phone settings: • Assign a softkey template. • Add a 14-button expansion module (optional). • Assign the phone button template. • Add a primary line. • Add shared lines for each configured manager. (Use the same DN and partition for the assistant secondary line and manager primary line.) • Add incoming intercom line (optional). • Add speed dial to the incoming intercom line for each configured manager (optional). • Set user locale. • Reset the phone. **Tip** To automatically configure some assistant phone settings, choose the Automatic Configuration check box on the User Information window when you are configuring the assistant. For more information, see the "Assistant Phones" section on page 3-14.	Manager and Assistant Phone Configuration, page 3-13 Finding a Phone, *Cisco CallManager Administration Guide* Deleting a Phone, *Cisco CallManager Administration Guide* Directory Number Configuration Overview, *Cisco CallManager Administration Guide* Configuring Speed-Dial Buttons, *Cisco CallManager Administration Guide* Resetting a Phone, *Cisco CallManager Administration Guide*
Step 9	Configure Cisco IP Manager Assistant: • Create a new manager. • Configure shared lines for manager. • Assign an assistant to a manager. • Configure lines for the assistant. • Intercom lines (optional)	Configuring a Manager and Assigning an Assistant for Shared Line Mode, page 3-16 Deleting Cisco IPMA Information for the Manager, page 3-17 Configuring Shared and Incoming Intercom Lines for the Assistant, page 3-18
Step 10	Configure the dial rules for the assistant.	Perform the following procedure to add a new dial rule or update an existing dial rule. See Application Dial Rules Configuration Error Checking in the Cisco CallManager System Guide for dial rule design and error checking., *Cisco CallManager Administration Guide*
Step 11	Install the Assistant Console application.	Installing the Assistant Console Application, page 3-22
Step 12	Configure the manager and assistant console applications.	*Cisco IP Manager Assistant User Guide*

Setting the Service Parameters for Cisco IPMA

Service Parameters for the Cisco IPMA service comprise three categories: general, clusterwide, and clusterwide parameters that must be configured if you want to use the IPMA automatic configuration for managers and assistants. Specify clusterwide parameters once for all Cisco IPMA services. Specify general parameters for each Cisco IPMA service that is installed.

Set the Cisco IPMA service parameters by using Cisco CallManager Administration to access the service parameters (**System > Service Parameters**). Choose the server where the Cisco IPMA application resides and then choose the Cisco IP Manager Assistant service.

Cisco IPMA includes the following service parameters that must be configured:

- Clusterwide Parameters That Apply to All Servers
  - Cisco IPMA Server (Primary) IP Address—No default. Administrator must manually enter this IP address.
  - Cisco IPMA Server (Backup) IP Address—No default. Administrator must manually enter this IP address.
  - Cisco IPMA Server Port—Default specifies Port 2912.
  - Cisco IPMA Assistant Console Heartbeat Interval—Default specifies 30 seconds. This interval timer specifies how long it takes for the failover to occur on the assistant console.
  - Cisco IPMA Assistant Console Request Timeout—Default specifies 30 seconds.
  - Cisco IPMA RNA Forward Calls—Default specifies False. This service parameter does not apply to shared line support.
  - Cisco IPMA RNA Timeout—Default specifies 10 seconds. This service parameter does not apply to shared line support.
  - CTIManager Connection Security Flag—This service parameter indicates whether security for Cisco IPMA service CTIManager connection is enabled or disabled. If enabled, Cisco IPMA will open a secure connection to CTIManager by using the Application CAPF profile that is configured in the CAPF Profile Instance Id for Secure Connection to CTIManager service parameter.
- Cisco IPMA Service Parameters for each server configured
  - CTIManager (Primary) IP Address—No default. Enter the IP address of the primary CTIManager that will be used for call control.
  - CTIManager (Backup) IP Address—No default. Administrator must manually enter this IP address.
  - Route Point Device Name for Proxy Mode—Not applicable for shared line support.
  - CAPF Profile Instance Id for Secure Connection to CTIManager—This service parameter specifies the Instance Id of the Application CAPF Profile for the Application User IPMASecureSysUser that this Cisco IPMA server will use to open a secure connection to CTIManager. You must configure this parameter if CTIManager Connection Security Flag is enabled.

Cisco IPMA includes the following clusterwide parameters that must be configured if you want to use the IPMA automatic configuration for managers and assistants:

- Clusterwide Parameters for Softkey Templates
  - Assistant Softkey Template—Default specifies Standard IPMA Assistant softkey template. This parameter specifies the softkey template that is assigned to the assistant device during IPMA assistant automatic configuration.
  - Manager Softkey Template for Proxy Mode—This service parameter does not apply to shared line support.
  - Manager Softkey Template for Shared Mode—Default specifies Standard Shared Mode Manager. Set this parameter to specify the shared mode softkey template that is assigned to the manager device during IPMA manager automatic configuration.

- IPMA Device Configuration Defaults for Proxy Mode—These parameters do not apply for IPMA with shared line support.
- Proxy Directory Number Range for Proxy Mode—These parameters do not apply for IPMA with shared line support.
- Proxy Directory Number Prefix for Proxy Mode—These parameters do not apply for IPMA with shared line support.

Security Considerations

Cisco IPMA supports a secure connection to CTI (transport layer security connection).

The administrator must configure a CAPF profile (one for each IPMA node) by choosing **User Management > Application User CAPF Profile**. From the Application User drop-down list box that is on the Application User CAPF Profile Configuration window, the administrator chooses IPMASecureSysUser.

For more information about configuring security for IPMA, see the information on the CTIManager Connection Security Flag and the CAPF Profile Instance Id for Secure Connection to CTIManager service parameters in the "Setting the Service Parameters for Cisco IPMA" section on page 3-11.

The *Cisco CallManager Security Guide* provides detailed security configuration procedures for CTI applications.

Starting the Cisco IPMA Service

Cisco IPMA service runs as an application on Cisco Tomcat. To start or stop the Cisco IPMA service, use the Serviceability Control Center Feature Services window.

Manager and Assistant Phone Configuration

You must configure and associate devices for each IPMA manager and assistant. Before you begin, complete the following tasks, depending on the phone type.

Cisco IP Phone Model 7940/41, 7960/61 and Model 7970/71

- Add a Cisco IP Phone model 7940/41, 7960/61 or model 7970/71 for each manager and assistant that will be using Cisco IPMA. To add these phones, use one of the following methods:
  - Manually (**Device > Phone**).
  - Auto registration
  - BAT
- Assign the Standard IPMA Assistant phone button template.

Cisco IP Phone Model 7940/41

You can use the Cisco IP Phone model 7940/41 for IPMA, but certain restrictions apply:

- Add a Cisco IP Phone model 7940/41 for each manager with the following items configured:
  - Two lines, one for the primary line and one for the intercom
  - Speed dial to the assistant intercom

  - Softkey template for manager with shared line support
- Add a Cisco IP Phone model 7940/41 for each assistant with the following items configured:
  - Two lines, one for the primary line and one for the intercom
  - Speed dial to the manager intercom
  - Softkey template for assistant

Note Cisco supports the Cisco IP Phone model 7940/41 for IPMA but recommends the Cisco IP Phone model 7960/61 or Cisco IP Phone model 7970/71 because they provide more functionality.

After you complete these tasks, configure the phones as described in the following sections:

- Manager Phones, page 3-14
- Assistant Phones, page 3-14
- Nonmanager and Nonassistant Phones, page 3-15

Manager Phones

The following section describes the IPMA requirements and tips for configuring a manager phone.

Manager Phone Configuration

Configure the manager Cisco IP Phones with the following settings:

- Standard IPMA Shared Mode Manager softkey template (must include the Immediate Divert and Transfer to Voice Mail soft keys)
- Primary line
- Additional lines for shared line support (optional)
- Voice-mail profile on primary line
- Incoming intercom line to support the auto answer with speakerphone or headset option (optional)
- Speed dial for outgoing intercom targets (optional)
- User locale

You can automate some of these settings by choosing the Automatic Configuration check box on the End User Configuration window when you configure the manager. For step-by-step instructions, see the "Configuring a Manager and Assigning an Assistant for Shared Line Mode" section on page 3-16.

Automatic Configuration sets the following items for the manager device or device profile:

- Softkey template
- Auto answer with speakerphone for intercom line

IPMA supports the Cisco IP Phone Model 7940/41. For more information, see the "Cisco IP Phone Model 7940/41" section on page 3-13.

Assistant Phones

The following section describes the IPMA requirements for configuring an assistant phone and provides tips on configuring an assistant phone. For step-by-step instructions, see the "Configuring Shared and Incoming Intercom Lines for the Assistant" section on page 3-18.

Assistant Phone Configuration

Configure the assistant Cisco IP Phones with the following settings:

- Standard IPMA Assistant softkey template (must include the Immediate Divert and Transfer to Voice Mail soft keys)
- Default 14-button expansion module (optional)
- Standard IPMA Assistant phone button template
- Primary line
- Shared lines for each configured manager (Use the same DN and partition as the manager primary line.)
- Incoming intercom line to support the auto answer with speakerphone or headset option
- Speed dial to incoming intercom line for each configured manager
- User locale

IPMA supports the Cisco IP Phone Model 7940/41. For more information, see the "Cisco IP Phone Model 7940/41" section on page 3-13.

Nonmanager and Nonassistant Phones

In addition to configuring manager and assistant devices, configure all other users in the Cisco CallManager cluster. Proper configuration allows managers and assistants to make calls to and receive calls from all other users in the cluster. No special configuration requirements exists in shared line support for nonmanager and nonassistant user phones.

Manager and Assistant Configuration

From the Cisco CallManager End User Configuration window, configure the settings for the managers and assistants who use the Cisco IPMA feature. From this window, perform the following functions:

- Choose manager and assistant devices.
- Automatically configure a manager or assistant device, if desired.
- Set up primary and incoming intercom lines for intercom capability. For example, extension 3102 serves as the intercom line for the manager. This line will receive intercom calls from the assistant. The assistant line 1 (1102) and line 2 (1103) display on the console, and the assistant answers them.
- Configure assistants for managers.
- Choose the local language in which the End User Configuration window displays.

The following sections provide details about configuring the manager and assistant settings:

- Configuring a Manager and Assigning an Assistant for Shared Line Mode, page 3-16
- Deleting Cisco IPMA Information for the Manager, page 3-17
- Deleting the Cisco IPMA Information for the Assistant, page 3-20
- Configuring Shared and Incoming Intercom Lines for the Assistant, page 3-18

Configuring a Manager and Assigning an Assistant for Shared Line Mode

Perform the following procedure to configure a Cisco IPMA manager and assign an assistant to the manager. To configure a new user and associate the device to the user, see "Adding an End User" in the *Cisco CallManager Administration Guide*. To configure the same directory number for the manager primary line and assistant secondary line, see "Directory Number Configuration Overview" in the *Cisco CallManager Administration Guide.*

Tip Configure Cisco IPMA manager information before configuring Cisco IPMA information for an assistant.

Procedure

Step 1 To configure the IPMA manager and to assign an assistant to an existing user, choose **User Management > End User**. From the Find and List Users window, click the **Find** button. The window displays all of the end users that are configured in Cisco CallManager.

Step 2 To display user information for the chosen manager, click the user name.

The End User Configuration window displays.

Step 3 To configure IPMA information for the manager, choose **Cisco IPMA Manager** from the Related Links drop-down list box and click **Go**.

Step 4 The Cisco IPMA Manager Configuration window displays and contains Manager information, Assistant information, and IPMA-controlled lines.

Step 5 To automatically configure the softkey template and auto answer with speakerphone for intercom line for the manager phone based on the IPMA service parameters, check the **Automatic Configuration** check box.

Step 6 Click the Uses Shared Lines check box.

Step 7 To associate a device name or device profile with a manager, choose the device name or device profile from the Device Name/Profile drop-down list box. (Extension mobility uses device profiles.) For information about using Cisco CallManager Extension Mobility with Cisco IPMA, see the "Extension Mobility" section on page 3-6.

Note If the manager telecommutes, click the Mobile Manager check box and optionally choose Device Profile. When Device Profile is chosen, the manager must log on to the phone by using extension mobility before accessing IPMA.

Step 8 From the Intercom Line drop-down list box, choose the intercom line appearance for the manager, if applicable.

Step 9 To assign an assistant to the manager, click the assistants name from the Available Assistants list and move it to the Associated Assistants list box by clicking the down arrow.

Tip You can go to the Cisco IPMA Assistant Configuration window by highlighting the assistant name and clicking the **Edit Assistant** link.

Step 10 To configure the IPMA controlled lines, click the appropriate line from the Available Lines list box and move it to the Selected Lines list box by clicking the down arrow.

Note Ensure the IPMA-controlled line is always the shared line DN.

To remove a line from the Selected Lines selection box and from Cisco IPMA control, highlight the line and click the up arrow.

Step 11 Click the **Save** button.

If you checked the Automatic Configuration check box and the service parameters are invalid, a message displays.

Upon successful completion of the automatic configuration, the manager device resets. If you configured a device profile, the manager must log out and log in to the device for settings to take effect.

Note When non-IPMA changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco IPMA and log in before the changes occur.

Additional Information

See the "Related Topics" section on page 3-23.

Deleting Cisco IPMA Information for the Manager

Perform the following procedure to delete Cisco IPMA information for a manager. To delete non-IPMA information for a manager, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Procedure

Step 1 To search for the manager for whom you want to delete IPMA information, choose **User Management > End User** from Cisco CallManager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all of the end users that are configured in Cisco CallManager.

Step 3 From the Find and List Users window, choose the manager whose Cisco IPMA information you want to delete. The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose **Cisco IPMA Manager** and click **Go**.

The Cisco IPMA Manager Configuration window displays for the user that you chose.

Step 5 Click the **Delete** button.

The update takes effect immediately.

Additional Information

See the "Related Topics" section on page 3-23.

Updating the Manager Cisco IPMA Configuration

Perform the following procedure to update Cisco IPMA information for a manager. To update non-IPMA information for a manager, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Procedure

Step 1 To search for the manager for whom you want to update IPMA information, choose **User Management > End User** from Cisco CallManager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all of the end users that are configured in Cisco CallManager.

Step 3 From the Find and List Users window, choose the manager whose Cisco IPMA information you want to update. The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose **Cisco IPMA Manager** and click **Go**.

The Cisco IPMA Manager Configuration window displays for the user that you chose.

Step 5 Update the information that you want changed such as device name, IPMA-controlled lines, or intercom line appearance.

Step 6 Click the **Save** button.

The update takes effect immediately.

Note The system automatically configures the softkey template and auto answer with speakerphone for intercom line for the manager phone on the basis of the IPMA service parameters when the Automatic Configuration check box is checked.

Note When non-IPMA changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco IPMA and log in for the changes to occur.

Additional Information

See the "Related Topics" section on page 3-23.

Configuring Shared and Incoming Intercom Lines for the Assistant

Use the Cisco IPMA Assistant Configuration of the End User Configuration window to configure the following items:

- Device name of the assistant phone
- Intercom line that the assistant uses to answer the manager calls (optional)
- Shared line of the manager to which the assistant phone gets associated (this gets done automatically when the manager and assistant share the same DN).

Administrators can set up one or more lines with a shared line appearance. The Cisco CallManager system considers a directory number to be a shared line if it appears on more than one device in the same partition.

In a shared line appearance, for example, you can set up a shared line, so a directory number appears on line 1 of a manager phone and also on line 2 of an assistant phone.

Perform the following procedure to configure the manager shared line and incoming intercom line appearances for an assistant. To configure a new user and associate devices, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Tip Before configuring the Cisco IPMA information for an assistant, you must configure the Cisco IPMA manager information and assign an assistant to the manager. See "Configuring a Manager and Assigning an Assistant for Shared Line Mode" section on page 3-16.

Procedure

Step 1 To search for the assistant for whom you want to update IPMA information, choose **User Management > End User** from Cisco CallManager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all the end users that are configured in Cisco CallManager.

Step 3 To display user information for the chosen assistant, click the user name.

The End User Configuration window displays.

Step 4 To configure IPMA information for the assistant, choose **Cisco IPMA Assistant** from the Related Links drop-down list box and click **Go**.

The Cisco IPMA Assistant Configuration window displays for the user that you chose.

Step 5 From the Device Name drop-down list box, choose the device name to associate with the assistant.

Step 6 From the Intercom Line drop-down list box, choose the incoming intercom line appearance for the assistant.

Tip To view existing manager configuration information, highlight the manager name in the Associated Managers list and click the **Edit Manager** link. The Cisco IPMA Manager Configuration window displays. To return to the Cisco IPMA Assistant Configuration window, highlight the assistant name and click the **Edit Assistant** link on the Cisco IPMA Manager Configuration window.

In the Associated Manager selection list box, the name of the previously configured IPMA manager displays.

Note The system automatically sets the softkey template and intercom line on the basis of the Cisco IPMA service parameter settings when the Automatic Configuration check box is checked. Additionally, the system sets auto answer with speakerphone for intercom line.

Step 7 To associate the manager line to the assistant line, perform the following steps from the Manager Association to the Assistant Line selection box:

a. In the Available Lines drop-down list box, choose the assistant line that will be associated with the manager line.

b. In the Manager Names drop-down list box, choose the preconfigured manager name with which the assistant is associated.

c. In the Manager Lines drop-down list box, choose the manager line that will be associated with the assistant line.

Step 8 Click the **Save** button.

The update takes effect immediately. If you chose automatic configuration, the assistant device automatically resets.

Additional Information

See the "Related Topics" section on page 3-23.

Deleting the Cisco IPMA Information for the Assistant

Perform the following procedure to delete Cisco IPMA information for an assistant. To delete non-IPMA information for an assistant, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Procedure

Step 1 To search for the assistant for whom you want to delete IPMA information, choose **User Management > End User** from Cisco CallManager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all the end users that are configured in Cisco CallManager.

Step 3 From the Find and List Users window, choose the assistant whose Cisco IPMA information you want to delete. The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose **Cisco IPMA Assistant** and click **Go**.

The Cisco IPMA Assistant Configuration window displays for the user that you chose.

Step 5 Click the **Delete** button.

The update takes effect immediately.

Note When non-IPMA changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco IPMA and log in before the changes occur.

Additional Information

See the "Related Topics" section on page 3-23.

Updating the Assistant Cisco IPMA Configuration

Perform the following procedure to update Cisco IPMA information for an assistant. To update non-IPMA information for an assistant, see the "Adding an End User" section in the *Cisco CallManager Administration Guide*.

Procedure

Step 1 To search for the assistant for whom you want to update IPMA information, choose **User Management > End User** from Cisco CallManager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all the end users that are configured in Cisco CallManager.

Step 3 From the Find and List Users window, choose the assistant whose Cisco IPMA information you want to update. The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose **Cisco IPMA Assistant** and click **Go**.

The Cisco IPMA Assistant Configuration window displays for the user that you chose.

Step 5 Update the information that you want changed such as device name, intercom line, or associated manager information.

Step 6 Click the **Save** button.

The update takes effect immediately.

Note During automatic configuration, the system automatically sets the softkey template and intercom line on the basis of the IPMA service parameter settings and sets auto answer with speakerphone for intercom line. If you do not want to use automatic configuration, uncheck the **Automatic Configuration** check box.

Note When non-IPMA changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco IPMA and log in before the changes occur.

Additional Information

See the "Related Topics" section on page 3-23.

Dial Rules Configuration

The administrator uses dial rules configuration to add and sort the priority of dialing rules. Dial rules for Cisco IPMA automatically strip numbers from or add numbers to telephone numbers that the assistant dials. For example, a dial rule can automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

The following sections provide additional information on application dial rules:

- Application Dial Rules Configuration Design, *Cisco CallManager System Guide*
- Application Dial Rules Configuration Error Checking, *Cisco CallManager System Guide*

Providing Information to Cisco IPMA Managers and Assistants

Install the assistant console application for Cisco IPMA by accessing a URL. The administrator sends the URL, in the "Installing the Assistant Console Application" section on page 3-22, to the assistant.

Note The assistant console application installation program supports Netscape 7.1 or later and Microsoft Internet Explorer 6.0 or later.

Installing the Assistant Console Application

Note When upgrading from Cisco CallManager release 4.0 or 4.1, you must reinstall the Assistant Console application.

Begin the installation by accessing the following URL:

https://<IPMA server>:8443/ma/Install/IPMAConsoleInstall.jsp

where

IPMA server specifies the IP address of the server that has the IPMA service running on it.

Tip You can localize the installer (with the proper localization pack) by including the proper parameter on the URL; for example, for French, you would include the following parameter at the end of the URL:?locale=fr_FR.

Assistant Console Dialog Options

The assistant console displays a dialog that contains the following options:

- Location to Install—The path of the directory where the assistant console software gets installed. The default specifies following path:

  c:\Program Files\Cisco\IPMA Assistant Console\

- Create Desktop Shortcut—Default specifies true. This parameter determines whether a shortcut is created on the assistant console.
- Create StartMenu Shortcut—Default specifies true. This parameter determines whether a shortcut is created in the Start menu (**Start > Programs > Cisco IPMA > IPMA Assistant Console**).
- Install JRE—Default specifies true. This parameter determines whether JRE is installed along with IPMA assistant console. If this option is turned off, you need to ensure that the following configuration is on the assistant console:
  - Install JRE 1.4.2_05 (international version) on the assistant console
  - Create an environment variable—IPMA_JRE on the assistant console, which gives the path to the JRE; for example, c:\Program Files\Jave\j2re1.4.2_05

Manager Configuration

Managers can customize their feature preferences from the Manager Configuration window by using the following URL:

https://<IPMA server>:8443/ma/desktop/maLogin.jsp

where

IPMA server specifies the IP address of the server that has the Cisco IPMA service running on it.

Note The Manager Configuration only supports Microsoft Internet Explorer 6.0 or later.

The administrator must send this URL to the manager.

Additional Information

See the "Related Topics" section on page 3-23.

Related Topics

- Cisco IP Manager Assistant With Proxy Line Support
- Softkey Templates, *Cisco CallManager System Guide*
- Understanding Directory Numbers, *Cisco CallManager System Guide*
- Directory Number Configuration Overview, *Cisco CallManager Administration Guide*
- Cisco IPMA Service, page 3-2
- Cisco IP Phone Interface, page 3-4
- Manager and Assistant Phone Configuration, page 3-13
- Nonmanager and Nonassistant Phones, page 3-15
- Configuring a Manager and Assigning an Assistant for Shared Line Mode, page 3-16
- Deleting Cisco IPMA Information for the Manager, page 3-17
- Updating the Manager Cisco IPMA Configuration, page 3-18
- Configuring Shared and Incoming Intercom Lines for the Assistant, page 3-18
- Deleting the Cisco IPMA Information for the Assistant, page 3-20
- Adding an End User, *Cisco CallManager Administration Guide*
- Associating Devices to an End User, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Manager Assistant User Guide*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *CDR Analysis and Reporting Administration Guide*

- *Cisco CallManager Bulk Administration Guide*
- *Cisco CallManager Security Guide*

Cisco Call Back

This chapter provides information on the following topics:

- Introducing Cisco Call Back, page 4-1
- Understanding How Cisco Call Back Works, page 4-2
- Suspend/Resume Functionality for Call Back, page 4-4
- System Requirements for Cisco Call Back, page 4-4
- Interactions and Restrictions, page 4-5
- Installing and Configuring Cisco Call Back, page 4-6
- Configuration Checklist for Cisco Call Back, page 4-7
- Providing Cisco Call Back Information to Users, page 4-10
- Troubleshooting Cisco Call Back, page 4-10
- Related Topics, page 4-10

Introducing Cisco Call Back

The Cisco Call Back feature allows you to receive call-back notification on your Cisco IP Phone when a called party line becomes available. You can activate call back for a destination phone that is within the same Cisco CallManager cluster as your phone or on a remote PINX over QSIG trunks or QSIG-enabled intercluster trunks.

To receive call-back notification, a user presses the CallBack softkey while receiving a busy or ringback tone. A user can also activate call back during reorder tone, which is triggered when the no answer timer expires.

The following sections provide information on the Cisco Call Back feature:

- Understanding How Cisco Call Back Works, page 4-2
- System Requirements for Cisco Call Back, page 4-4
- Interactions and Restrictions, page 4-5
- Installing and Configuring Cisco Call Back, page 4-6

Understanding How Cisco Call Back Works

The following examples describe how Cisco Call Back works after an unavailable phone becomes available:

- Example: User A calls user B, who is not available, page 4-2
- Example: User A calls user B, who configured Call Forward No Answer (CFNA) to user C before call back activation occurs, page 4-3
- Example: User A calls user B, who configures call forwarding to user C after user A activates call back, page 4-3
- Example: User A and user C call user B at the same time, page 4-3

Note The calling phone only supports one active call back request. The called phone can support multiple call back requests.

Cisco Call Back only supports spaces and digits 0 through 9 for the name or number of the calling or called party. To work with Cisco Call Back, the name or number of the calling or called party cannot contain # or * (pound sign or asterisk).

Note If the originating side (User A) gets reset after Cisco Call Back has been activated, then Call Back gets automatically cancelled. User A does not receive an audio alert and the Callback notification screen does not display. If the terminating side (User B) gets reset, Call Back does not get cancelled. User A will receive an audio alert and the Callback notification screen displays after User B becomes available.

Example: User A calls user B, who is not available

User A calls user B, who exists either in the same Cisco CallManager cluster as user A or in a different cluster. Because user B is busy or does not reply, user A activates the Call Back feature by using the Callback softkey. The following call back activation message displays on the phone of user A:

```
CallBack is activated on <DN of User B>
Press Cancel to deactivate
Press Exit to quit this screen
```

User A presses the Exit softkey.

After user B becomes available (phone becomes on hook after busy or completes an off-hook and on-hook cycle from idle), user A receives an audio alert, and the following message displays on the phone of User A:

```
<DN of User B> has become available
Time HH:MM MM/DD/YYYY
Press Dial to call
Press Cancel to deactivate
Press Exit to quit this screen
```

User A presses the Exit softkey and then goes off hook and dials the DN of User B. User B answers the call. User A and User B go on hook.

When User A presses the Callback softkey, the following message displays on the phone of User A:

```
<DN of User B> has become available
Time HH:MM MM/DD/YYYY
Press Dial to call
Press Cancel to deactivate
Press Exit to quit this screen
```

Note Manually dialing a DN that has been activated with Cisco Call Back notification has no effect on the Cisco Call Back status.

Example: User A calls user B, who configured Call Forward No Answer (CFNA) to user C before call back activation occurs

The following scenario applies to Call Forward No Answer.

The call from user A gets forwarded to user C because Call Forward No Answer is configured for user B. User A uses call back to contact user C if user C is not busy; if user C is busy, user A contacts user B.

When user B or user C becomes available (on hook), user A receives an audio alert, and a message displays on user A phone that states that the user is available.

Example: User A calls user B, who configures call forwarding to user C after user A activates call back

The following scenarios support Call Forward All, Call Forward Busy, and Call Forward No Answer.

- User A calls user B, who exists in the same Cisco CallManager cluster as user A. Use A activates call back because user B is not available. Before user B becomes available to user A, user B sets up call forwarding to user C. User A may call back user B or user C, depending on the call forwarding settings for user B.
- User A calls user B, who exists in a different cluster. The call connects by using a QSIG trunk. User A activates call back because user B is not available. Before user B becomes available to user A, user B sets up call forwarding to user C. One of the following events occurs:
  - If the Callback Recall Timer (T3) has not expired, user A always calls back User B.
  - After the Callback Recall Timer (T3) expires, user A may call back user B or user C, depending on the call forwarding settings of user B.

Tip The timer starts when the system notifies user A that user B is available. If user A does not complete the call back call during the allotted time, the system cancels call back. On the phone of user A, a message states that user B is available, even after the call back cancellation. User A can dial user B.

Example: User A and user C call user B at the same time

User A and user C call user B at the same time, and user A and user C activate call back because user B is unavailable. A call back activation message displays on the phones of user A and user C.

When user B becomes available, both user A and user C receive an audio alert, and a message displays on both phones that states that user B is available. The user, that is, user A or user C, that presses the Dial softkey first connects to user B.

Suspend/Resume Functionality for Call Back

Cisco Call Back provides the ability of the system to suspend the call completion service if the user, who originated Cisco Call Back, is currently busy and receives call-back notification when the called party becomes available. When the originating user then becomes available, the call completion service resumes for that user.

After the originating user (User A) activates the Cisco Call Back feature, and then becomes busy when the called party (User B) becomes available, the originating PINX sends out a Suspend Callback APDU message indicating to the peer to suspend monitoring of User B until User A becomes available again. When User A becomes available, the originating PINX sends the Resume APDU message for the terminating side to start monitoring User B again.

Note Cisco Call Back supports the originating Suspend/Resume call-back notification for both intracluster and intercluster QSIG trunks or QSIG-enabled intercluster trunks. It also supports Suspend/Resume notification for QSIG-enabled H.225 trunks, and H.323 gateways.

The following example describes how the Suspend/Resume feature works:

Example: User A is busy when User B becomes available

User A calls user B, who exists either in the same Cisco CallManager cluster as user A or in a different cluster. Because user B is busy or does not reply, user A activates the Call Back feature by using the Callback softkey. The following call back activation message displays on the phone of user A:

```
CallBack is activated on <DN of User B>
Press Cancel to deactivate
Press Exit to quit this screen
```

User A presses the Exit softkey.

User A has a busy trigger set to 1.

User A becomes busy. User B then becomes available.

User A does not receive an audio alert and does not receive a call-back notification screen on the display.

The originating side (User A) sends a Suspend Callback APDU message to the terminating side (User B).

User A becomes available. The originating side sends a Resume Callback APDU message to the terminating side. This causes monitoring of User B to resume.

When User B becomes available, User A receives an audio alert and a Callback notification screen displays.

System Requirements for Cisco Call Back

Cisco Call Back requires the following software components:

- Cisco CallManager 5.0 or later
- Cisco CallManager service running on at least one server in the cluster
- Cisco Database Layer Monitor service running on the same server as the Cisco CallManager service
- Cisco RIS Data Collector service running on the same server as the Cisco CallManager service

- Cisco IP Telephony Locale Installer, that is, if you want to use non-English phone locales or country-specific tones
- Microsoft Internet Explorer or Netscape Navigator

Interactions and Restrictions

Note If users want the Cisco Call Back softkeys and messages on the phone to display in any language other than English, or if you want the user to receive country-specific tones for calls, install the locale installer, as described in the Cisco IP Telephony Locale Installer documentation.

Cisco IP Phone models 7970, 7960, 7940, 7912, 7905 and Cisco Communicator support Cisco Call Back with the CallBack softkey (can be calling and called phone). You can use call back with some Cisco-provided applications, such as Cisco IP Manager Assistant (IPMA).

Note The only Session Initiation Protocol (SIP) phone that support Cisco Call Back are the Cisco IP Phone model s7970, 7971, 7961, and 7941.

You can call the following devices and can have call back activated on them:

- Cisco IP Phone 30 SP+, Cisco IP Phone 12 SP+, Cisco IP Phone 12 SP, Cisco IP Phone 12 S, Cisco IP Phone 30 VIP
- Cisco IP Phone 7902, Cisco IP Phone 7910, Cisco IP Phone 7935, Cisco IP Phone 7936
- Cisco VGC Phone (uses the Cisco VG248 Gateway)
- Cisco Skinny Client Control Protocol (SCCP) Phone models 7971, 7970, 7961, and 7941
- Cisco Session Initiation Protocol (SIP) Phone models 7970, 7971, 7961, and 7941
- Cisco Analog Telephone Adapter (ATA) 186 and 188
- CTI route point forwarding calls to above phones

Tip When a Cisco CallManager Extension Mobility user logs in or logs out, any active call completion that is associated with call back automatically gets canceled. If a called phone is removed from the system after call back is activated on the phone, the caller receives reorder tone after pressing the Dial softkey. The user may cancel or reactivate call back.

If you forward all calls to voice-messaging system, you cannot activate call back.

Additional Information on Cisco Call Back Notification with SIP Phones

The way that call back notification works on the SIP 7960 and 7940 phones differs from the SCCP phone models. The Cisco SIP Phone models 7960 and 7940 do not support call back notification for on-hook/off-hook states. The only way that Cisco CallManager would know when a line on a SIP 7960 or 7940 phone becomes available is by monitoring an incoming SIP INVITE message that Cisco CallManager receives from the phone. After the phone sends SIP INVITE to Cisco CallManager and the phone goes on hook, Cisco CallManager will be able to send an audio and call back notification screen the SIP 7960/7940 user.

Feature Interactions with Call Forward, iDivert, and Voice-Messaging System Features

The following call states describe the expected behaviors, for the calling party, that occur when Cisco CallManager Call Back interacts with the Call Forward, iDivert, and voice-messaging system features.

When a called party (Phone B) either forwards an incoming call using Forward All, Forward Busy, or Forward No Answer; or diverts a call using iDivert; to a voice-messaging system, the calling party (Phone A) can enter one of the following states with respect to the call back feature:

- VM-Connected state: The call gets connected to voice-messaging system. The Call Back softkey remains inactive on the calling party's (Phone A) phone.
- Ring-Out state with the original called party: The voice-mail profile of the called party does not have a voice-mail pilot. The called party (Phone B) will see "Key Is Not Active" after pressing the iDivert softkey. The calling party (Phone A) should be able to activate call back against the original called party (Phone B).
- Ring-Out state with voice-messaging system feature and voice-mail pilot number as the new called party: The call encounters either voice-messaging system failure or network failure. The called party (Phone B) will see "Temp Failure" after pressing iDivert softkey. The calling party (Phone A) cannot activate call back against the original called party (Phone B) because the call context has the voice mail pilot number as the "new" called party.
- Ring-Out state with busy voice-mail port and voice-mail pilot number as the new called party: The call encounters busy voice-mail port. The called party (Phone B) will see "Busy" after pressing iDivert softkey. The calling party (Phone A) cannot activate call back against the original called party (Phone B) because the call context has the voice mail pilot number as the "new" called party.

For more information refer to the following sections:

- Phone Features, *Cisco CallManager System Guide*
- Immediate Divert, page 11-1

Installing and Configuring Cisco Call Back

Cisco Call Back automatically installs when you install Cisco CallManager. After you install Cisco CallManager, you must configure Cisco Call Back in Cisco CallManager Administration, so phone users can use the Cisco Call Back feature.

For successful configuration of the Cisco Call Back feature, review the steps in the configuration checklist, perform the configuration requirements, and activate the Cisco CallManager service. The following sections provide detailed configuration information:

- Configuration Checklist for Cisco Call Back, page 4-7
- Creating a Softkey Template for the CallBack Softkey, page 4-7
- Configuring CallBack Softkey Template in Device Pool, page 4-8
- Adding CallBack Softkey Template in Phone Configuration, page 4-9
- Setting Cisco Call Back Service Parameters, page 4-9

Configuration Checklist for Cisco Call Back

Table 4-1 shows the steps for configuring the Cisco Call Back feature.

Table 4-1 Cisco Call Back Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	If phone users want the softkeys and messages to display in a language other than English, or if you want the user to receive country-specific tones for calls, verify that you installed the locale installer.	Cisco IP Telephony Locale Installer documentation
Step 2	In Cisco CallManager Administration, create a copy of the Standard User softkey template and add the CallBack softkey to the following states: • On Hook call state • Ring Out call state • Connected Transfer call state	Creating a Softkey Template for the CallBack Softkey, page 4-7
Step 3	In Cisco CallManager Administration, add the new softkey template to the device pool.	Configuring CallBack Softkey Template in Device Pool, page 4-8
Step 4	In the Phone Configuration window, perform one of the following tasks: • Choose the device pool that contains the new softkey template. • Choose the new softkey template from the Softkey Template drop-down list box.	Adding CallBack Softkey Template in Phone Configuration, page 4-9
Step 5	In the Phone Configuration window, verify that the correct user locale is configured for the Cisco IP Phone(s).	End User Configuration Settings, *Cisco CallManager Administration Guide* Phone Configuration Settings, *Cisco CallManager Administration Guide* Cisco IP Telephony Locale Installer documentation
Step 6	If you do not want to use the default settings, configure the Cisco Call Back service parameters.	Setting Cisco Call Back Service Parameters, page 4-9
Step 7	Verify that the Cisco CallManager service is activated in Cisco CallManager Serviceability.	*Cisco CallManager Serviceability Administration Guide*

Creating a Softkey Template for the CallBack Softkey

Perform the following procedure to create a new softkey template with the CallBack softkey.

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Device Settings > Softkey Template**.

The Softkey Template Configuration window displays.

Step 2 From the Find and List Softkey Template window, choose the Standard User softkey template.

Step 3 Click the **Copy** icon.

The Softkey Template Configuration window displays with new information.

Step 4 In the Softkey Template Name field, enter a new name for the template; for example, Standard User for Call Back.

Step 5 Click the **Save** button.

The Softkey Template Configuration redisplays with new information.

Step 6 To add the CallBack softkey to the template, choose **Configure Softkey Layout** from the Related Links drop-down list box in the upper, right corner and click **Go**.

The Softkey Layout Configuration window displays. You must add the CallBack softkey to the On Hook, Ring Out, and Connected Transfer call states.

Step 7 To add the CallBack softkey to the On Hook call state, choose **On Hook** from the Select a Call State to Configure drop-down list box.

The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 8 From the Unselected Softkeys list, choose the CallBack softkey and click the right arrow to move the softkey to the Selected Softkeys list.

Step 9 To save and continue, click the **Save** button.

Step 10 To add the CallBack softkey to the Ring Out call state, choose **Ring Out** from the Select a Call State to Configure drop-down list box.

The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 11 From the Unselected Softkeys list, choose the CallBack softkey and click the right arrow to move the softkey to the Selected Softkeys list.

Step 12 To save and continue, click the **Save** button.

Step 13 To add the Call Back softkey to the **Connected Transfer** call state, choose Connected Transfer from the Select a Call State to Configure drop-down list box.

Step 14 The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 15 From the Unselected Softkeys list, choose the Call Back softkey and click the right arrow to move the softkey to the Selected Softkeys list.

Step 16 Click the **Save** button.

Configuring CallBack Softkey Template in Device Pool

Perform the following procedure to add the Call Back softkey template to the device pool. You can add the template to the default device pool if you want all users to have access to the CallBack softkey, or you can create a customized device pool for Call Back feature users.

Procedure

Step 1 From Cisco CallManager Administration, choose **System > Device Pool**.

The Find and List Device Pool window displays.

Step 2 Choose the Default device pool or any previously created device pool that is in the Device Pools list.

Step 3 In the Softkey Template field, choose the softkey template that contains the CallBack softkey from the drop-down list box. (If you have not created this template, see the "Creating a Softkey Template for the CallBack Softkey" section on page 4-7.)

Step 4 Click the **Save** button.

A dialog box displays with a message to press Reset to update the device pool settings.

Adding CallBack Softkey Template in Phone Configuration

Perform the following procedure to add the Call Back softkey template to each user phone.

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Phone**.

The Find and List Phones window displays.

Step 2 Find the phone to which you want to add the softkey template. See Finding a Phone in the *Cisco CallManager Administration Guide*.

Step 3 Perform one of the following tasks:

- From the Device Pool drop-down list box, choose the device pool that contains the new softkey template.
- In the Softkey Template drop-down list box, choose the new softkey template that contains the CallBack softkey.

Step 4 Click the **Save** button.

A dialog box displays with a message to press Reset to update the phone settings.

Setting Cisco Call Back Service Parameters

You configure Cisco Call Back service parameters by accessing **Service > Service Parameters** in Cisco CallManager Administration; choose the server where the Cisco CallManager service runs and then choose the Cisco CallManager service.

Unless instructed otherwise by the Cisco Technical Assistance Center, Cisco recommends that you use the default service parameters settings. Cisco Call Back includes service parameters such as Callback Enabled Flag, Callback Audio Notification File Name, Connection Proposal Type, Connection Response Type, Call Back Request Protection T1 Timer, Callback Recall T3 Timer, Callback Calling Search Space, No Path Preservation, and Set Private Numbering Plan for Callback. For information on these parameters, click the question mark button that displays in the upper corner of the Service Parameter window.

Providing Cisco Call Back Information to Users

The *Cisco IP Phone Models 7960 and 7940 User Guide* provides procedures for how to use the Call Back feature on the Cisco IP Phone. Use this guide in conjunction with the question mark button help that displays on the phone.

Troubleshooting Cisco Call Back

Use the Cisco CallManager Serviceability Trace Configuration and Real-Time Monitoring Tool to help troubleshoot call back problems. Refer to the *Cisco CallManager Serviceability Administration Guide*.

Additional Information

See the "Related Topics" section on page 4-10.

Related Topics

- Softkey Template Configuration, *Cisco CallManager Administration Guide*
- Device Defaults Configuration, *Cisco CallManager Administration Guide*
- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager System Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Troubleshooting Guide for Cisco CallManager*
- *Cisco IP Phones Model 7960 and 7940 User Guide*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- Cisco IP Telephony Locale Installer

CHAPTER 5

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 Forced Authorization Codes regulate the types of calls that certain users can place.

Client matter codes force the user to enter a code to specify that the call relates to a specific client matter. You can assign client matter codes to customers, students, or other populations for call accounting and billing purposes. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

The CMC and FAC features require that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled FAC and/or CMC for each route pattern.

This chapter contains information on the following topics:

- Introducing Client Matter Codes, page 5-2
- Introducing Forced Authorization Codes, page 5-2
- Interactions and Restrictions, page 5-3
- System Requirements, page 5-5
- Installation of CMC and FAC, page 5-5
- CMC and FAC Configuration Checklist, page 5-5
- Client Matter Codes Configuration, page 5-6
- CMC Configuration Settings, page 5-8
- Enabling Client Matter Codes For Route Patterns, page 5-8
- Forced Authorization Codes Configuration, page 5-9
- FAC Configuration Settings, page 5-11
- Enabling Forced Authorization Codes for Route Patterns, page 5-12
- Providing Information to Users, page 5-13
- Using CDR Analysis and Reporting (CAR), page 5-4
- Related Topics, page 5-13

Introducing Client Matter Codes

To use the Client Matter Codes feature, users must enter a client matter code to reach certain dialed numbers. You enable or disable CMC through route patterns, and you can configure multiple client matter codes. When a user dials a number that is routed through a CMC-enabled route pattern, a tone prompts the user for the client matter code. When the user enters a valid CMC, the call occurs; if the user enters an invalid code, reorder occurs. The CMC writes to the CDR, so you can collect the information by using CDR Analysis and Reporting (CAR), which generates reports for client accounting and billing.

The Client Matter Codes feature benefits law offices, accounting firms, consulting firms, and other businesses or organizations where tracking the length of the call for each client is required. Before you implement CMC, obtain a a list of all clients, groups, individuals, parties, and so on that you plan to track through CMC. Determine whether you can assign the codes consecutively, arbitrarily, or whether your organization requires a special code structure; for example, using existing client account numbers for CMC. For each client (or group, individual, and so on) that you want to track, you must add a client matter code in the Client Matter Code Configuration window of Cisco CallManager Administration. Then, in Cisco CallManager Administration, you must enable CMC for new or existing route patterns. After you configure CMC, make sure that you update your dial plan documents to indicate the CMC-enabled route patterns.

Tip If you want users to enter a CMC for most calls, consider enabling CMC for most or all route patterns in the dial plan. In this situation, users must obtain CMCs and a code, such as 555, for calls that do not relate to clients. All calls automatically prompt the users for a CMC, and the users do not have to invoke CMC or dial special digits. For example, a user dials a phone number, and the system prompts the user for the client code; if the call relates to a client matter, the user enters the appropriate CMC; if the call does not relate to a client, the user enters 555.

If only a select number of users must enter a CMC, consider creating a new route pattern specifically for CMC; for example, use 8.@, which causes the system to prompt users for the client code when the phone number that is entered starts with the number 8. Implementing CMC in this manner provides a means to invoke CMC and allows the existing dial plan to remain intact. For example, for client-related calls, a user may dial 8-214-555-1234 to invoke CMC; for general calls that are not related to clients, the users just dial 214-555-1234 as usual.

Introducing Forced Authorization Codes

When you enable FAC through route patterns in Cisco CallManager Administration, users must enter an authorization code to reach the intended recipient of the call. When a user dials a number that is routed through a FAC-enabled route pattern, the system plays a tone that prompts for the authorization code.

In Cisco CallManager Administration, you can configure various levels of authorization. If the user authorization code does not meet or exceed the level of authorization that is specified to route the dialed number, the user receives a reorder tone. If the authorization is accepted, the call occurs. The name of the authorization writes to call detail records (CDRs), so you can organize the information by using CDR Analysis and Reporting (CAR), which generates reports for accounting and billing.

You can use FAC for colleges, universities, or any business or organization when limiting access to specific classes of calls proves beneficial. Likewise, when you assign unique authorization codes, you can determine which users placed calls. For each user, you specify an authorization code, then enable FAC for relevant route patterns by selecting the appropriate check box and specifying the minimum authorization level for calls through that route pattern. After you update the route patterns in Cisco CallManager Administration, update your dial plan documents to define the FAC-enabled route patterns and configured authorization level.

To implement FAC, you must devise a list of authorization levels and corresponding descriptions to define the levels. You must specify authorization levels in the range of 0 to 255. Cisco allows authorization levels to be arbitrary, so you define what the numbers mean for your organization. Before you define the levels, review the following considerations, which represent examples or levels that you can configure for your system:

- Configure an authorization level of 10 for interstate long-distance calls in North America.
- Because intrastate calls often cost more than interstate calls, configure an authorization level of 20 for intrastate long-distance calls in North America.
- Configure an authorization level of 30 for international calls.

Tip Incrementing authorization levels by 10 establishes a structure that provides scalability when you need to add more authorization codes.

Interactions and Restrictions

You can implement CMC and FAC separately or together. For example, you may authorize users to place certain classes of calls, such as long distance calls, and also assign the class of calls to a specific client. If you implement CMC and FAC together as described in the previous example, the user dials a number, enters the user-specific authorization code when prompted to do so, and then enters the client matter code at the next prompt. CMC and FAC tones sound the same to the user, so the feature tells the user to enter the authorization code after the first tone and enter the CMC after the second tone.

Cisco CallManager provides redundancy, which handle the normal processes that are in place for Cisco CallManager.

The CMC and FAC features work with all Cisco IP Phone models and MGCP-controlled analog gateways.

Before you implement CMC and FAC, review the following restrictions:

- After dialing the phone number, hearing-impaired users should wait 1 or 2 seconds before entering the authorization or client matter code.
- Calls that are forwarded to a FAC- or CMC-enabled route pattern fail because no user is present to enter the code. This limitation applies to call forwarding that is configured in Cisco CallManager Administration or the Cisco CallManager User Options Pages. You can configure call forwarding, but all calls that are forwarded to a FAC- or CMC-enabled route pattern results in reorder. When a user presses the CFwdALL softkey and enters a number that has FAC or CMC enabled on the route pattern, the user receives reorder, and call forwarding fails.

  You cannot prevent the configuration of call forwarding to a FAC- or CMC-enabled route pattern; forwarded calls that use these route patterns drop because no code is entered. To minimize call-processing interruptions, test the number before you configure call forwarding. To do this, dial the intended forwarding number; if you are prompted for a code, do not configure call forwarding for that number. Advise users of this practice to reduce the number of complaints that result from forwarded calls that do not reach the intended destination.
- Cisco does not localize FAC or CMC. The CMC and FAC features use the same default tone for any locale that is supported with Cisco CallManager.

- The CMC and FAC features do not support overlap sending because the Cisco CallManager cannot determine when to prompt the user for the code. If you check the Require Forced Authorization Code or the Require Client Matter Code check box on the Route Pattern Configuration window, the Allow Overlap Sending check box becomes disabled. If you check the Allow Overlap Sending check box, the Require Forced Authorization Code and the Require Client Matter Code check boxes become disabled.
- The FAC and CMC tones can only be played on SCCP phones, TAPI/JTAPI ports, and MGCP FXS ports.
- H.323 analog gateways do not support FAC or CMC because these gateways cannot play tones.
- Restrictions apply to CTI devices that support FAC and CMC. For more information, see the "Using FAC/CMC with CTI, JTAPI, and TAPI Applications" section on page 5-4.
- Cisco WebDialer does not support FAC or CMC.
- Cisco IP SoftPhone cannot play tones; however, after a Cisco SoftPhone user dials a directory number, the user can use CMC and FAC by waiting 1 or 2 seconds before entering the code.
- If you do not append the FAC or CMC with #, the system waits for the T302 timer to extend the call.
- When you press the Redial softkey on the phone, you must enter the authorization code or CMC when the number that you dialed is routed through a FAC- or CMC-enabled route pattern. Cisco does not save the code that you entered for the previous call.
- You cannot configure authorization code or CMC for speed-dial buttons. You must enter the code when the system prompts you to do so.

Using the Cisco Bulk Administration Tool (BAT)

You can use BAT to insert, update, and delete CMC and FAC. For more information on how to perform these tasks, refer to the *Cisco CallManager Bulk Administration Guide* that is compatible with this release of Cisco CallManager.

Using CDR Analysis and Reporting (CAR)

CDR Analysis and Reporting (CAR) allows you to run reports that provide call details for authorization code names, authorization levels, and CMCs. For information on how to generate reports in CAR, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Using FAC/CMC with CTI, JTAPI, and TAPI Applications

In most cases, Cisco CallManager can alert a CTI, JTAPI, or TAPI application that the user must enter a code during a call. When a user places a call, creates an ad hoc conference, or performs a consult transfer through a FAC- or CMC-enabled route pattern, the user must enter a code after receiving the tone. When a user redirects or blind transfers a call through a FAC- or CMC-enabled route pattern, the user receives no tone, so the application must send the codes to Cisco CallManager. If Cisco CallManager receives the appropriate codes, the call connects to the intended party. If Cisco CallManager does not receive the appropriate codes, Cisco CallManager sends an error to the application that indicates which code is missing.

Cisco CallManager does not support call forwarding through FAC- or CMC-enabled route patterns. For more information, see the "Interactions and Restrictions" section on page 5-3.

System Requirements

The minimum requirements for CMC and FAC specify that every server in the cluster must have Cisco CallManager 5.0.

Installation of CMC and FAC

The CMC and FAC features install automatically when you install Cisco CallManager. To make these features work in your Cisco CallManager network, you must perform the tasks that are described in the "CMC and FAC Configuration Checklist" section on page 5-5.

CMC and FAC Configuration Checklist

Use Table 5-1 as a guide when you configure CMC and FAC.

Table 5-1 Cisco CMC and FAC Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Review feature limitations.	Interactions and Restrictions, page 5-3
Step 2	Design and document the system; for example, document a list of client matters that you want to track.	Introducing Client Matter Codes, page 5-2 Introducing Forced Authorization Codes, page 5-2
Step 3	Insert the codes by using Cisco CallManager Administration or by using Cisco Bulk Administration Tool (BAT). **Tip** Consider using BAT for small or large batches of codes; the comma separated values (CSV) file in BAT can serve as a blueprint for the codes, corresponding names, corresponding levels, and so on.	Client Matter Codes Configuration, page 5-6 Forced Authorization Codes Configuration, page 5-9
Step 4	To enable FAC or CMC, add or update route patterns in Cisco CallManager Administration.	Enabling Client Matter Codes For Route Patterns, page 5-8 Enabling Forced Authorization Codes for Route Patterns, page 5-12
Step 5	Update your dial plan documents or keep a printout of the BAT CSV file with your dial plan documents.	Refer to your dial plan documents.
Step 6	Provide all necessary information, for example, codes, to users and explain how the features works.	Providing Information to Users, page 5-13

Client Matter Codes Configuration

After you obtain the list of CMCs that you plan to use, you add those codes to the database and enable the CMC feature for route patterns.

This section contains the information on the following topics:

- Finding Client Matter Codes, page 5-6
- Configuring Client Matter Codes, page 5-7
- Deleting Client Matter Codes, page 5-8
- CMC Configuration Settings, page 5-8
- Enabling Client Matter Codes For Route Patterns, page 5-8
- Providing Information to Users, page 5-13

Finding Client Matter Codes

Cisco CallManager lets you locate specific CMCs on the basis of specific criteria. To locate CMCs, perform the following procedure:

Note During your work in a browser session, Cisco CallManager Administration retains your search preferences. If you navigate to other menu items and return to this menu item, Cisco CallManager Administration retains your search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Client Matter Codes**.

The Find and List window displays.

Tip To find all CMCs that are registered in the database, click **Find** without entering any search text.

Step 2 From the first Find Client Matter Codes where drop-down list box, choose one option; for example, Client Matter Code or Description.

Note The criterion that you choose in the first drop-down list box specifies how the list that your search generates will be sorted. For example, if you choose Client Matter Code, the Client Matter Code column displays as the left column of the results list.

Step 3 From the second Client Matter Codes where drop-down list box, choose one option; for example, begins with, contains, ends with, is exactly, and so on.

Step 4 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

Note You can delete multiple client matter codes from the Find and List window by checking the check boxes next to the appropriate CMC and clicking **Delete Selected**. You can delete all CMC in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 5 From the list of records, click the CMC that you want to display.

The window displays the CMC that you choose.

Additional Information

See the "Related Topics" section on page 5-13.

Configuring Client Matter Codes

You enter CMCs in Cisco CallManager Administration or through the Cisco Bulk Administration Tool (BAT). If you use BAT, the BAT comma separated values (CSV) file provides a record of CMCs and client names. After you configure CMC, make sure that you update your dial plan documents or keep a printout of the BAT CSV file with your dial plan documents.

To add or update CMCs in Cisco CallManager Administration, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- To add CMCs, choose **Call Routing > Client Matter Codes** and click **Add New**. Continue with Step 2.
- To update CMCs, locate the CMC that you want to update, as described in the "Finding Client Matter Codes" section on page 5-6 and continue with Step 2.

Step 2 Enter the appropriate settings as described in Table 5-2.

Step 3 Click **Save**.

Step 4 After you add all CMCs, see the "Enabling Client Matter Codes For Route Patterns" section on page 5-8.

Additional Information

See the "Related Topics" section on page 5-13.

Deleting Client Matter Codes

To delete a CMC in Cisco CallManager Administration, perform the following procedure:

Procedure

Step 1 Locate the CMC that you want to delete, as described in the "Finding Client Matter Codes" section on page 5-6.

Step 2 After the Client Code Matter Configuration window displays, click **Delete**.

Step 3 To continue with the deletion, click **OK**.

Additional Information

See the "Related Topics" section on page 5-13.

CMC Configuration Settings

Use Table 5-2 in conjunction with the "Configuring Client Matter Codes" section on page 5-7.

Table 5-2 Configuration Settings for Adding a CMC

Setting	Description
Client Matter Code	Enter a unique code of no more than 16 digits that the user will enter when placing a call. The CMC displays in the CDRs for calls that use this code.
Description	Enter a name of no more than 50 characters. This optional field associates a client code with a client.

Additional Information

See the "Related Topics" section on page 5-13.

Enabling Client Matter Codes For Route Patterns

Perform the following steps to enable CMCs on route patterns:

Procedure

Step 1 In Cisco CallManager Administration, choose **Call Routing > Route/Hunt > Route Pattern**.

Step 2 Perform one of the following tasks:

- To update an existing route pattern, enter search criteria in the Find and List Route Pattern window, as described in "Route Pattern Configuration" in the *Cisco CallManager Administration Guide*.
- To add a new route pattern, refer to "Route Pattern Configuration" in the *Cisco CallManager Administration Guide*.

Step 3 In the Route Pattern Configuration window, check the **Require Client Matter Code** check box.

Step 4 Perform one of the following tasks:

- If you updated the route pattern, click **Save**.
- If you added a new route pattern, click **Save**.

Step 5 Repeat Step 2 through Step 4 for all route patterns that require a client matter code.

Step 6 After you complete the route pattern configuration, see the "Providing Information to Users" section on page 5-13.

Additional Information

See the "Related Topics" section on page 5-13.

Forced Authorization Codes Configuration

To configure FACs, see the following sections:

- CMC and FAC Configuration Checklist, page 5-5
- Finding Forced Authorization Codes, page 5-9
- Configuring Forced Authorization Codes, page 5-10
- Deleting Forced Authorization Codes, page 5-11
- FAC Configuration Settings, page 5-11
- Providing Information to Users, page 5-13
- Enabling Forced Authorization Codes for Route Patterns, page 5-12

Finding Forced Authorization Codes

Cisco CallManager allows you to locate specific FACs on the basis of specific criteria. To locate FACs, perform the following procedure:

Note During your work in a browser session, Cisco CallManager Administration retains your search preferences. If you navigate to other menu items and return to this menu item, Cisco CallManager Administration retains your search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Forced Authorization Codes**.

The Find and List window displays.

Tip To find all authorization codes that are registered in the database, click **Find** without entering any search text.

Step 2 From the first Find Authorization Codes where drop-down list box, choose one option; for example, Authorization Code Name, Authorization Code, or Authorization Code Level.

Note The criterion that you choose in the first drop-down list box specifies how the list that your search generates will be sorted. For example, if you choose Authorization Code Name, the Authorization Code Name column displays as the left column of the results list.

Step 3 From the second Find Authorization Codes where drop-down list box, choose one option; for example, begins with, contains, ends with, is exactly, and so on.

Step 4 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

Note You can delete multiple authorization codes from the Find and List window by checking the check boxes next to the appropriate FAC and clicking **Delete Selected**. You can delete all FAC in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 5 From the list of records, click the authorization code that you want to display.

The window displays the FAC that you choose.

Additional Information

See the "Related Topics" section on page 5-13.

Configuring Forced Authorization Codes

After you design your FAC implementation, you enter authorization codes either in Cisco CallManager Administration or through the Cisco Bulk Administration Tool (BAT). Consider using BAT for large batches of authorization codes; the comma separated values (CSV) file in BAT serves as a blueprint for authorization codes, corresponding names, and corresponding levels.

Note For future reference, make sure that you update your dial plan documents or keep a printout of the CSV file with your dial plan documents.

To add a small number of authorization codes in Cisco CallManager Administration, perform the steps in the following procedure.

Procedure

Step 1 In Cisco CallManager Administration, choose **Call Routing > Forced Authorization Codes**.

Step 2 Perform one of the following tasks:

- To add a new FAC, click **Add New**.
- To update an FAC, locate the authorization code that you want to update as described in the "Finding Forced Authorization Codes" section on page 5-9.

Step 3 Using the configuration settings in Table 5-3, configure the authorization codes.

Step 4 Click **Save**.

Note After you add all authorization codes, see the "Enabling Forced Authorization Codes for Route Patterns" section on page 5-12.

Additional Information

See the "Related Topics" section on page 5-13.

Deleting Forced Authorization Codes

To delete a FAC, perform the following procedure:

Procedure

Step 1 Locate the authorization code that you want to delete, as described in the "Finding Forced Authorization Codes" section on page 5-9.

Step 2 After the Forced Authorization Code Configuration window displays, click **Delete**.

Step 3 To continue with the deletion, click **OK**.

Additional Information

See the "Related Topics" section on page 5-13.

FAC Configuration Settings

Use Table 5-3 in conjunction with the "Configuring Forced Authorization Codes" section on page 5-10.

For more information, see the "Related Topics" section on page 5-13.

Table 5-3 Configuration Settings for FAC

Setting	Description
Authorization Code Name	Enter a unique name that is no more than 50 characters. This name ties the authorization code to a specific user or group of users; this name displays in the CDRs for calls that use this code.

Table 5-3 Configuration Settings for FAC (continued)

Setting	Description
Authorization Code	Enter a unique authorization code that is no more than 16 digits. The user enters this code when the user places a call through a FAC-enabled route pattern.
Authorization Level	Enter a three-digit authorization level that exists in the range of 0 to 255; the default equals 0. The level that you assign to the authorization code determines whether the user can route calls through FAC-enabled route patterns. To successfully route a call, the user authorization level must equal or be greater than the authorization level that is specified for the route pattern for the call.

Additional Information

See the "Related Topics" section on page 5-13.

Enabling Forced Authorization Codes for Route Patterns

Perform the following steps to enable FACs for route patterns:

Procedure

Step 1 In Cisco CallManager Administration, choose **Call Routing > Route/Hunt > Route Pattern**.

Step 2 Perform one of the following tasks:

- To update an existing route pattern, enter search criteria in the Find and List Route Pattern window, as described in "Route Pattern Configuration" in the *Cisco CallManager Administration Guide*.
- To add a new route pattern, refer to "Route Pattern Configuration" in the *Cisco CallManager Administration Guide*.

Step 3 In the Route Pattern Configuration window, check the **Require Forced Authorization Code** check box.

Step 4 Click **Save**.

Tip Even if you do not check the Require Forced Authorization Code check box, you can specify the authorization level because the database stores the number that you specify.

Step 5 Repeat Step 2 through Step 4 for all route patterns that require an authorization code.

Step 6 After you complete the route pattern configuration, see the "Providing Information to Users" section on page 5-13.

Additional Information

See the "Related Topics" section on page 5-13.

Providing Information to Users

After you configure the feature(s), communicate the following information to your users:

- Inform users about restrictions that are described in "Interactions and Restrictions" section on page 5-3.
- Provide users with all necessary information to use the features; for example, authorization code, authorization level, client matter code, and so on. Inform users that dialing a number produces a tone that prompts for the codes.
- For FAC, the system attributes calls that are placed with the user authorization code to the user or the user department. Advise users to memorize the authorization code or to keep a record of it in a secure location.
- Advise users of the types of calls that users can place; before a user notifies a phone administrator about a problem, users should hang up and retry the dialed number and code.
- Inform users that they can start entering the code before the tone completes.
- To immediately route the call after the user enters the code, the users can press # on the phone; otherwise, the call occurs after the interdigit timer (T302) expires; that is, after 15 seconds by default.
- The phone plays a reorder tone when the user enters an invalid code. If users misdial the code, the user must hang up and try the call again. If the reorder tone persists, users should notify the phone or system administrator that a problem may exist with the code.

Additional Information

See the "Related Topics" section on page 5-13.

Related Topics

- Route Pattern Configuration, *Cisco CallManager Administration Guide*
- Understanding Route Plans, *Cisco CallManager System Guide*
- Interactions and Restrictions, page 5-3
- System Requirements, page 5-5

Forced Authorization Codes

- Introducing Forced Authorization Codes, page 5-2
- CMC and FAC Configuration Checklist, page 5-5
- Finding Forced Authorization Codes, page 5-9
- Configuring Forced Authorization Codes, page 5-10
- Deleting Forced Authorization Codes, page 5-11
- FAC Configuration Settings, page 5-11
- Enabling Forced Authorization Codes for Route Patterns, page 5-12

Client Matter Codes

- Introducing Client Matter Codes, page 5-2
- CMC and FAC Configuration Checklist, page 5-5

- Finding Client Matter Codes, page 5-6
- Configuring Client Matter Codes, page 5-7
- Deleting Client Matter Codes, page 5-8
- CMC Configuration Settings, page 5-8
- Enabling Client Matter Codes For Route Patterns, page 5-8

Additional Cisco Documentation

- *Cisco CallManager Bulk Administration Guide*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Serviceability Administration Guide*

CHAPTER 6

Music On Hold

The integrated Music On Hold (MOH) feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. The Music On Hold feature allows two types of hold:

- End-user hold
- Network hold, which includes transfer hold, conference hold, and call park hold

Music On Hold also supports other scenarios where recorded or live audio is needed.

This chapter covers the following topics:

- Understanding Music On Hold, page 6-1
- Music On Hold Server, page 6-8
- Music On Hold Audio Sources, page 6-8
- Music On Hold System Requirements and Limits, page 6-12
- Music On Hold Failover and Fallback, page 6-13
- Music On Hold Configuration Checklist, page 6-14
- Monitoring Music On Hold Performance, page 6-15
- Additional Information, page 6-16
- Fixed Music On Hold Audio Source Configuration, page 6-21
- Music On Hold Server Configuration, page 6-23
- Related Topics, page 6-28

Understanding Music On Hold

The following sections explain the Music On Hold feature by providing definitions, service characteristics, feature functionality with examples, and supported features.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Definitions

In the simplest instance, music on hold takes effect when phone A is talking to phone B, and phone A places phone B on hold. If Music On Hold (MOH) resource is available, phone B listens to music that is streamed from a music on hold server.

The following definitions provide important information for the discussion that follows:

- MOH server—A software application that provides music on hold audio sources and connects a music on hold audio source to a number of streams.
- Media resource group—A logical grouping of media servers. You may associate a media resource group with a geographical location or a site as desired. You can also form media resource groups to control server usage or desired service type (unicast or multicast).
- Media resource group list—A list that comprises prioritized media resource groups. An application can select required media resources from among ones that are available according to the priority order that is defined in a media resource group list.
- Audio source ID—An ID that represents an audio source in the music on hold server. The audio source can be either a file on a disk or a fixed device from which a source stream music on hold server obtains the streaming data. One cluster can support up to 51 audio source IDs (1 to 51). Each audio source (represented by an audio source ID) can stream as unicast and multicast mode, if needed.
- Holding party—In an active, two-party call, the party that initiates a hold action (either user hold or network hold). Example: if party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party A is the holding party.
- Held party—In an active, two-party call, the party that does not initiate a hold action but is involved. Example: if party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party B is the held party.

The following audio source ID selection rules apply for selecting audio source IDs and media resource group lists:

- The system administrator, not the end user, defines (configures) audio source IDs.
- The system administrator chooses (configures) audio source IDs for device(s) or device pool(s).
- Holding parties define which audio source ID applies to held parties.
- Cisco CallManager implements four levels of prioritized audio source ID selection with level four as highest priority and level one as lowest priority.
  - The system selects audio source IDs at level four, which is directory/line-based, if defined. (Devices with no line definition, such as gateways, do not have this level.)
  - If no audio source ID is defined in level four, the system searches any selected audio source IDs in level three, which is device based.
  - If no level four nor level three audio source IDs are selected, the system selects audio source IDs that are defined in level two, which is DevicePool-based.
  - If all higher levels have no audio source IDs selected, the system searches level one for audio source IDs, which are clusterwide parameters.

The following media resource group list selection rules apply:

- Held parties determine the media resource group list that a Cisco CallManager uses to allocate a music on hold resource.
- Two levels of prioritized media resource group list selection exist:
  - Level two media resource group list provides the higher priority level, which is device based. Cisco CallManager uses the media resource group list at the device level if such a media resource group list is defined.
  - Level one media resource group list provides the lower priority level, which is an optional DevicePool parameter. Cisco CallManager uses the DevicePool level media resource group list only if no media resource group list is defined in the device level for that device.
- If no media resource group lists are defined, Cisco CallManager uses the system default resources. System default resources comprise resources that are not assigned to any existing media resource group. System default resources are always unicast.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Characteristics

The integrated Music On Hold feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. This source makes music available to any possible on-net or off-net device that is placed on hold. On-net devices include station devices and applications that are placed on hold, consult hold, or park hold by an interactive voice response (IVR) or call distributor. Off-net users include those who are connected through Media Gateway Control Protocol (MGCP)/skinny gateways, IOS H.323 gateways and IOS Media Gateway Control Protocol gateways. The Music On Hold feature is also available for Cisco IP POTS phones that are connected to the Cisco IP network through FXS ports on IOS H.323/Media Gateway Control Protocol and for Cisco Media Gateway Control Protocol/skinny gateways.

The integrated Music On Hold feature covers media server, data base administration, call control, media resource manager, and media control functional areas.

The music on hold server provides the music resources/streams. These resources register with the Cisco CallManager during the initialization/recovery period.

Database administration provides a user interface to allow the Cisco CallManager administrator to configure the Music On Hold feature for the device(s). Database administration also provides Cisco CallManager call control with configuration information.

Call control controls the music on hold scenario logic.

The media resource manager processes the registration request from the music on hold server and allocates/deallocates the music on hold resources under the request of call control.

Media control controls the establishment of media stream connections, which can be one-way or two-way connections.

You must ensure that an end device is provisioned with music on hold-related information before music on hold functions for that device. Initializing a Cisco CallManager creates a media resource manager. The music on hold server(s) registers to the media resource manager with its music on hold resources.

When an end device or feature places a call on hold, Cisco CallManager connects the held device to a music resource. When the held device is retrieved, it disconnects from the music on hold resource and resumes normal activity.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Functionality

For music on hold to function, you must perform the actions in the following list:

- Configure music on hold servers.
- Configure audio sources. For the examples that follow, configure and provision the following audio sources: *Thank you for holding* and *Pop Music 1*.

Note Define audio sources first and then set up the music on hold servers, especially when multicast will be used. The user interface allows either step to take place first.

Note If an audio source is configured for multicast, the MOH server always transmits the audio stream, regardless of whether devices are held.

- Configure media resource groups. If multicast is desired, check the Use Multicast for MOH Audio check box.
- Configure media resource group lists.
- Assign media resource group lists and audio sources to device pools.
- Assign media resource group lists and audio sources to devices (to override assignments made to device pools).
- Assign audio sources to lines (to override device settings).

Using the preceding configuration actions, if you define music on hold functionality as follows, the examples that follow demonstrate music on hold functionality for user hold, transfer hold, and call park.

Media Resource Groups

MOH designates a music on hold server. MRG designates a media resource group.

- MRG_D comprises MOH_D.
- MRG_S_D comprises MOH_S and MOH_D.

Media Resource Group Lists

MRGL designates a media resource group list.

- MRGL_D comprises MRG_D.
- MRGL_S_D comprise MRG_S_D and MRG_D (prioritized order).

Nodes

- Dallas node comprises phone D and MOH_D.
- San Jose node comprises phone S and MOH_S.
- Assign phone D audio source ID 5, *Thank you for holding* or plain music (for both user and network hold), and MRGL_D.
- Assign phone S audio source ID 1, *Pop Music 1* (for both user and network hold), and MRGL_S_D.

User Hold Example

Phone D calls phone S, and phone S answers. Phone D presses the Hold softkey. Result: Phone S receives *Thank you for holding* announcement or plain music that is streaming from MOH_S. (MOH_S has available streams.) When phone D presses the Resume softkey, phone S disconnects from the music stream and reconnects to phone D.

Transfer Hold Example

Transfer hold serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone D presses the Transfer softkey. Phone S receives *Thank you for holding* announcement or plain music that is streaming from MOH_D. (MOH_S has no available streams, while MOH_D does.) After phone D completes the transfer action, phone S disconnects from the music stream and gets redirected to phone X, the transfer destination.

Call Park Example

Call park serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone S presses the CallPark softkey. Phone D receives a beep tone. (MOH_D has no available streams.) Phone X picks up the parked call. Phone S gets redirected to phone X (phone D and phone X are conversing).

Additional Information

See the "Related Topics" section on page 6-28.

Supported Music On Hold Features

Music on hold supports the following features, which are listed by category. Feature categories include music on hold server characteristics, server scalability, server manageability, server redundancy, database scalability, and manageability.

Music On Hold Server Characteristics

- Servers stream music on hold from music on hold data source files that are stored on their disks.
- Servers stream music on hold from an external audio source (for example, looping tape recorder, radio, or CD).
- Music on hold servers can use a single music on hold data source for all source streams and, hence, all connected streams. When multiple music on hold servers are involved, the local server of each music on hold server always stores the music on hold data source files. Cisco CallManager does not support distribution of fixed-device (hardware) audio sources across music on hold servers within a media resource group.
- Music on hold data source files have a common filename across all music on hold servers.
- Music on hold data source files must be uploaded to each server in the cluster.
- Each audio source receives a feed from either a designated file or a designated fixed source (for example, radio or CD).
- A designated fixed source comprises a single device, which is either enabled or disabled.

- The audio driver on the local machine makes a single fixed source available to the music on hold server.
- Music on hold servers support the G.711 (a-law and mu-law), G.729a, and wideband codecs.
- Music on hold servers register with one primary Cisco CallManager server.

Server Scalability

- Music on hold supports from 1 to 500 simplex unicast streams per music on hold server.
- Music on hold supports multiple Cisco-developed media-processing applications, including Interactive Voice Response (IVR) and AutoAttendant (AA). Cisco CallManager facilitates this support.
- Music on hold server simultaneously supports up to 50 music on hold data source files as sources.
- Music on hold server supports one fixed-device stream source in addition to the file stream sources. This source is the fixed audio source, which is configured on the Music On Hold (MOH) Fixed Audio Source Configuration page. This source requires the additional Cisco USB Music-On-Hold-capable adaptor.

Server Manageability

- From Cisco CallManager Serviceability windows, you can activate the music on hold server application, Cisco IP Media Streaming Application, on any standard media convergence server (MCS) as a service.
- You can activate music on hold application on the same media convergence server (MCS) as other media applications, so music on hold and the other media application(s) co-reside on the MCS.
- You can install music on hold server application on multiple media convergence servers (MCS) in a cluster.
- The administrator can specify the source for each source stream that is provided by the server.
- Administration of stream sources takes place through a browser.

Server Redundancy

- Music on hold servers support Cisco CallManager lists. The first entry on the list serves as the primary server, and subsequent Cisco CallManagers on the list serve as backup Cisco CallManagers in prioritized order.
- Music on hold servers can maintain a primary and backup connection to Cisco CallManagers from their Cisco CallManager list.
- Music on hold servers can re-home to backup Cisco CallManagers by following the standard procedures that are used by other servers and phones on the cluster.
- Music on hold servers can re-home to their primary server by following standard procedures for other media servers on the cluster.

Cisco CallManager/Database Requirements

- When a Cisco CallManager is handling a call and places either endpoint in the call on hold, the Cisco CallManager can connect the held endpoint to music on hold. This feature holds true for both network hold and user hold. Network hold includes transfer, conference, call park, and so forth.
- A media resource group for music on hold supports having a single music source stream for all connected streams.

- The system supports having music on hold server(s) at a central site without music on hold server(s) at remote sites. Remote site devices that require music on hold service can obtain service from a media resource group across the WAN when service is not available locally.
- You can distribute music on hold servers to any site within a cluster.
- A music on hold server can use a single music on hold data source for all source streams and, hence, all connected streams. When multiple music on hold servers are involved, the music on hold data source may be a file stored locally on each server.
- The system can detect when the primary media resource group that supplies music on hold for a device is out of streams and can select a stream from the secondary or tertiary media resource group that is specified for that device.
- When connecting a device to music on hold, the system can insert a transcoder when needed to support low-bandwidth codecs.

Database Scalability

- Cisco CallManager can support from 1 to 500 unicast sessions per music on hold server.
- A cluster can support from 1 to more than 20 music on hold servers.
- A cluster can support from 1 to more than 10,000 simultaneous music on hold streams across the cluster.
- A cluster can support from 1 to 500 or more media resource groups for music on hold.
- A media resource group for music on hold can support from 1 to 20 or more music on hold servers.

Manageability

- The administrator can select media resource group list per device.
- The administrator can select music on hold source stream per device/DN.
- The administrator can select music on consult (network hold) source stream per device/DN.
- The administrator can configure which music on hold servers are part of a specified media resource group.
- The administrator can designate a primary, secondary, and tertiary music on hold/consult servers for each device by configuring media resource groups and media resource group lists.
- The administrator can provision multiple music on hold servers.
- The administrator can provision any device registered with the system such that any music on hold server can service it in the system.
- All music on hold configuration and administration take place through a browser.
- The administrator specifies the user hold and network hold audio sources for each device pool. These default audio sources may be either file-based or fixed device-based.
- The administrator can designate a music on hold server as either unicast or multicast, provided that resources exist to support multicast.
- The administrator can reset all music on hold servers.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Server

The music on hold server uses the Station Stimulus (Skinny Client) messaging protocol for communication with Cisco CallManager. A music on hold server registers with the Cisco CallManager as a single device and reports the number of simplex, unicast audio streams that it can support. The music on hold server advertises its media type capabilities to the Cisco CallManager as G.711 mu-law and a-law, G.729a, and wideband. Cisco CallManager starts and stops music on hold unicast streams by sending skinny client messages to the music on hold server.

A music on hold server handles up to 500 simplex, unicast audio streams. A media resource group includes one or more music on hold servers. A music on hold server supports 51 audio sources, with one audio source that is sourced from a fixed device that uses the local computer audio driver, and the rest that are sourced from files on the local music on hold server.

You may use a single file for multiple music on hold servers, but the fixed device may be used as a source for only one music on hold server. The music on hold audio source files get stored in the proper format for streaming. Cisco CallManager allocates the simplex unicast streams among the music on hold servers within a cluster.

The music on hold server uses the media convergence server series hardware platform. A Cisco USB sound adaptor that is installed on the same computer as the music on hold server application provides the external fixed audio source, which can be a looping tape recorder, radio, or CD.

The music on hold server, which is actually a component of the Cisco IP Voice Media Streaming application, supports standard device recovery and database change notification.

Each music on hold server uses the local hard disk to store copies of the Music On Hold audio source files. Each audio source file gets distributed to the server(s) when the file is added through the Cisco CallManager Administration interface.

Note The administrator must upload Music On Hold audio source files to each MOH server.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Audio Sources

When the administrator imports an audio source file, the Cisco CallManager Administration window interface processes the file and converts the file to the proper format(s) for use by the music on hold server.

The recommended format for audio source files specifies the following:

- 16-bit PCM wav file
- Stereo or mono
- Sample rates of 48kHz, 32kHz, 16kYz, or 8kHz

Additional Information

See the "Related Topics" section on page 6-28.

Default Music On Hold Sample

Cisco CallManager includes a default music on hold sample that automatically downloads with Cisco CallManager software for customer use.

Additional Information

See the "Related Topics" section on page 6-28.

Creating Audio Sources

Most standard wav files serve as valid input audio source files, including the following file types:

- 16-bit PCM (stereo/mono)
- 8-bit CCITT a-law or mu-law (stereo/mono)

Note The Music On Hold feature does not support the MP3 format.

In creating an audio source, the following sequence takes place:

- The administrator imports the audio source file into the Cisco CallManager cluster. This step may take some time to transfer the file and convert the file to the proper format(s) for the music on hold server to use.
- The administrator must import the audio source file to the MOH server in each cluster prior to assigning an audio source number to the audio source file.
- The music on hold server uses the local audio source file(s).
- The music on hold server streams the files by using a kernel mode RTP driver as Cisco CallManager needs or requests.

Additional Information

See the "Related Topics" section on page 6-28.

Storing Audio Source Files

In previous releases, Cisco CallManager did not limit the amount of space that MOH files used. The MOH upload tool does not limit the number of uploaded files or the file size. The modified upload JSP pages check the disk usage of existing MOH files and only permit uploads if sufficient space is found.

The following considerations also apply:

- Release 5.0 of Cisco CallManager supports up to five MOH audio sources on 36- or 40-gigabyte disk-based systems. Systems with 72- or 80-gigabyte disks support the entire 50 audio streams.
- To increase the number of audio sources that Cisco CallManager supports, install a larger disk during upgrade.

Note The smallest node on the cluster controls MOH capacity.

Additional Information

See the "Related Topics" section on page 6-28.

Managing Audio Sources

After music on hold audio sources are created, their management occurs entirely through the Cisco CallManager Administration web interface. Choose **Media Resources > Music On Hold Audio Source** to display the Music On Hold (MOH) Audio Source Configuration window. For a given audio source, use this window to add, update, or delete a music on hold audio source. For each audio source file, assign a music on hold audio source number and music on hold audio source name and decide whether this audio source will play continuously and allow multicasting. For an audio source, this window also displays the music on hold audio source file status. Refer to the "Finding a Music On Hold Audio Source" section on page 6-17 for details.

Note Beginning with Release 5.0 of Cisco CallManager, the Music On Hold Audio Source Configuration window uploads audio source files only to a particular server. The window does not provide for automatic copying of audio source files to any other servers. You must manually upload audio source files to subscriber servers by accessing the Cisco CallManager application on each server.

Additional Information

See the "Related Topics" section on page 6-28.

Multicast and Unicast Audio Sources

Multicast music on hold conserves system resources. Multicast allows multiple users to use the same audio source stream to provide music on hold. Multicast audio sources associate with an IP address.

Unicast music on hold, the system default, uses a separate source stream for each user or connection. Users connect to a specific device or stream.

For administrators, multicast entails managing devices, IP addresses, and ports. In contrast, unicast entails managing devices only.

For multicast, administrators must define at least one audio source to allow multicasting. To define music on hold servers for multicast, first define the server to allow multicasting.

For multicast, an address comprises a combination of an IP address and a port number. Each audio source for multicast requires a set of addresses: one for each format on each MOH server. When configuring the MOH server for multicast, specify whether addresses should be assigned by incrementing the port or the IP address.

Caution Cisco strongly recommends incrementing 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.

The Max Hops field in the Music On Hold (MOH) Server Configuration window indicates the maximum number of routers that an audio source is allowed to cross. If max hops is set to zero, the audio source must remain in its own subnet. If max hops is set to one, the audio source can cross up to one router to the next subnet. Cisco recommends setting max hops to two.

A standards body reserves IP addresses. Addresses for IP multicast range from 224.0.1.0 to 239.255.255.255. The standards body, however, assigns addresses in the range 224.0.1.0 to 238.255.255.255 for public multicast applications. Cisco strongly discourages using public multicast addresses for music on hold multicast. Instead, Cisco recommends using an IP address in the range that is reserved for administratively controlled applications on private networks (239.0.0.0 to 239.255.255.255).

Valid port numbers for multicast include even numbers that range from 16384 to 32767. (The system reserves odd values.)

Multicast functions only if both media resource groups and media resource group lists are defined to include a multicast music on hold server. For media resource groups, you must include a music on hold server that is set up for multicast. Such servers are labeled as *(MOH)[Multicast]*. Also, check the Use Multicast for MOH Audio check box when defining a media resource group for multicast.

For media resource group lists, which are associated with device pools and devices, define the media resource group list, so the media resource group set up for multicast is the first group in the list. This recommended practice facilitates the device efforts to find the multicast audio source first.

In music on hold processing, the held device (the device placed on hold) determines the media resource to use, but the holding device (the device that initiates the hold action) determines the audio source to use.

Additional Information

See the "Related Topics" section on page 6-28.

Multicast Configuration Checklist

Table 6-1 provides a checklist for configuring various Cisco Call Manager services to allow multicasting. You must perform all steps for multicast to be available.

Table 6-1 Multicast Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Configure a music on hold server to enable multicast audio sources. ⚠ **Caution** Cisco strongly recommends incrementing multicast on IP address in firewall situations. This results in each multicast audio source having a unique IP address and helps to avoid network saturation.	Music On Hold Server Configuration Settings, page 6-26
Step 2	Configure an audio source to allow multicasting.	Music On Hold Audio Source Configuration Settings, page 6-19
Step 3	Create a media resource group and configure it to use multicast for MOH audio.	Media Resource Group Configuration Settings, *Cisco CallManager Administration Guide*

Table 6-1 Multicast Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 4	Create a media resource group list with a multicast media resource group as the primary media resource group.	Media Resource Group List Configuration Settings, *Cisco CallManager Administration Guide*
Step 5	Choose the media resource group list that was created in Step 4 for either a device pool or for specific devices.	Related Topics, *Cisco CallManager Administration Guide*

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold System Requirements and Limits

The following system requirements and limits apply to the Music On Hold feature:

- All audio streaming devices that are using the Music On Hold feature support simplex streams. The music on hold server supports up to 500 simplex streams.
- The music on hold (MOH) server, a part of the Cisco IP Voice Media Streaming application, gets installed with Cisco CallManager. Use the Cisco CallManager Serviceability application to activate the MOH server. Only one Cisco IP Voice Media Streaming application may be activated on a media convergence server, and therefore only one MOH server can be enabled per server. The Cisco IP Voice Media Streaming application, however, can be activated on multiple servers to provide multiple MOH servers for the cluster.
- For a Cisco CallManager cluster, you may define up to 50 audio sources. A Cisco CallManager Administration window supports import, addition, update, and deletion of each audio source. The music on hold server also supports one fixed input source. The system supports the following codecs: G.711 a-law/mu-law, G.729a, and wideband.

  Note Because the G.729a codec is designed for human speech, using it with music on hold for music may not provide acceptable audio quality.

- For each cluster, you may define up to 50 audio sources from files as well as one fixed audio source. A Cisco CallManager Administration window supports addition, update, and deletion of each audio source. All servers use local copies of the same 50 or fewer files. You must set up the fixed audio source that is configured per cluster on each server.
- For each cluster, you may define at most 20 music on hold servers. The Cisco CallManager Administration window allows import, addition, update, and deletion of music on hold servers. The window allows administrators to specify the following characteristics for each server:
  - Name
  - Node (server host name)
  - Device pool
  - Maximum number of unicast and multicast streams
  - Sources to multicast
  - For each multicast source: IP address, port, and time to live (maximum number of router hops)

- Cisco CallManager Administration allows definition of at least 500 media resource groups per cluster. Each media resource group may include any combination of at least 20 media resources, including music on hold servers, media termination points, transcoders, and conference devices. Music on hold servers in one cluster support at least 10,000 simultaneous music on hold streams. See "Media Resource Groups" in the *Cisco CallManager System Guide* for details of media resource groups.
- Cisco CallManager Administration allows definition of media resource group lists. See "Media Resource Group Lists" in the *Cisco CallManager System Guide* for details of media resource group lists.
- Modifications to the Cisco CallManager Administration device configuration windows for phones and gateways allow the selection of a media resource group list, hold stream source, and consult stream source as optional parameters for a device.
- Modifications to the Cisco CallManager Administration Directory Number configuration windows allow selection of a user hold source and a network hold source.
- Modifications to the Cisco CallManager Administration Service Parameters allows entry to a clusterwide, default music on hold stream source (default specifies 1) and default media resource group type (default specifies unicast).
- The number of streams that the music on hold server can use may decrease if the annunciator, software MTP, or software conference bridge is in use on the same MCS server.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Failover and Fallback

The music on hold server supports Cisco CallManager lists and failover as implemented by the software conference bridge and media termination point. Upon failover, the system maintains connections to a backup Cisco CallManager if one is available.

Cisco CallManager takes no special action when a music on hold server fails during an active music on hold session. The held party receives nothing from this point, but this situation does not affect normal call functions.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Configuration Checklist

Table 6-2 provides a checklist for configuring music on hold.

Table 6-2 Music On Hold Configuration Checklist

Configuration Steps		**Procedures and Related Topics**
Step 1	The Cisco IP Voice Media Streaming application gets installed automatically upon installation of Cisco CallManager. To provide an MOH server, you must use the Cisco CallManager Serviceability application to activate the Cisco IP Voice Media Streaming application. When a server gets added, the Cisco CallManager automatically adds the media termination point, conference bridge, annunciator, and music on hold devices to the database. **Note** During installation, Cisco CallManager installs and configures a default music on hold audio source if one does not exist. Music on hold functionality can proceed by using this default audio source without any other changes.	*Installing Cisco CallManager Release 5.0(1)*
Step 2	Run the music on hold audio translator. ⚠ **Caution** If the audio translator translates files on the same server as the Cisco CallManager, serious problems may occur. The audio translator tries to use all available CPU time, and Cisco CallManager may experience errors or slowdowns.	Music On Hold Audio Sources, page 6-8
Note	The installation program performs the following actions automatically. If the user manually adds the music on hold components, ensure the following steps are performed.	
Step 3	Configure the music on hold server.	Configuring a Music On Hold Server, page 6-24
Step 4	Add and configure audio source files.	Finding a Music On Hold Audio Source, page 6-17

Additional Information

See the "Related Topics" section on page 6-28.

Monitoring Music On Hold Performance

Perform the activities in Table 6-3 to monitor music on hold performance.

Table 6-3 Music On Hold Performance Monitoring

Monitoring Activity		Detailed Information
Step 1	Use the Cisco CallManager Serviceability Real-Time Monitoring Tool (RTMT) to check resource usage and device recovery state.	Viewing Music On Hold Server Performance, page 6-15 *Cisco CallManager Serviceability Administration Guide* and *Cisco CallManager Serviceability System Guide* document another method of viewing this information.
Step 2	Search the event log for Cisco IP Voice Media Streaming application entries.	*Cisco CallManager Serviceability Administration Guide* *Cisco CallManager Serviceability System Guide*
Step 3	Verify that the Cisco IP Voice Media Streaming application service is running.	Additional Information, page 6-16 *Cisco CallManager Serviceability Administration Guide* and *Cisco CallManager Serviceability System Guide* document another method of viewing this information.
Step 4	Search the Media Application trace (CMS) to see what music on hold-related activity that it detects.	*Cisco CallManager Serviceability Administration Guide* and *Cisco CallManager Serviceability System Guide*

Additional Information

See the "Related Topics" section on page 6-28.

Viewing Music On Hold Server Performance

To view music on hold server perfmon counters, use the Cisco CallManager Serviceability Real-Time Monitoring Tool (RTMT).

Table 6-4 details the performance monitoring counters that display in the Cisco CallManager Serviceability Real-Time Monitoring Tool Performance window.

Table 6-4 Music On Hold Performance Counters

Performance Counter Name	Description
MOHConnectionState	Indicates primary and secondary Cisco CallManager: • 1 = Primary • 2 = Secondary • 0 = Not connected
MOHAudioSourcesActive	Specifies total number of active audio sources, including each supported codec type. If audio Source 1 has mu-law and G.729 enabled, count for this audio source may show 2.
MOHStreamsActive	Specifies total number of active streams. Two potential overhead streams exist for each audio source/codec type: one for actual audio source, another for multicast.
MOHStreamsAvailable	Specifies total number of available simplex streams. Total represents total number of streams that are available in device driver for all devices.
MOHConnectionsLost	Specifies number of times that connection has been lost for the corresponding Cisco CallManager.
MOHStreamsTotal	Specifies total number of streams that are processed.

See the *Cisco CallManager Serviceability System Guide* for additional information about the Real-Time Monitoring Tool.

Additional Information

See the "Related Topics" section on page 6-28.

Checking Service States

To check whether the music on hold service is running, use Performance Management.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Audio Source Configuration

The integrated Music On Hold feature provides the ability to place on-net and off-net users on hold with music streamed from a streaming source. This feature includes the following actions:

- End user hold
- Network hold, which includes transfer hold, conference hold, and park hold

Music On Hold configuration comprises configuration of Music On Hold audio sources and Music On Hold servers.

Use the following topics to configure Music On Hold audio sources:

- Finding a Music On Hold Audio Source, page 6-17
- Configuring a Music On Hold Audio Source, page 6-18
- Deleting a Music On Hold Audio Source, page 6-19
- Music On Hold Audio Source Configuration Settings, page 6-19

Additional Information

See the "Related Topics" section on page 6-28.

Finding a Music On Hold Audio Source

Because you might have multiple Music On Hold audio sources in your network, Cisco CallManager lets you search for Music On Hold audio sources on the basis of specified criteria. Follow these steps to search for a specific Music On Hold audio source in the Cisco CallManager database.

Note During your work in a browser session, Cisco CallManager Administration retains your Music On Hold audio source search preferences. If you navigate to other menu items and return to this menu item, Cisco CallManager Administration retains your Music On Hold audio source search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Media Resources > Music On Hold Audio Source**.

The Find and List Music On Hold Audio Sources window displays.

Step 2 From the first drop-down list box, choose on the following criteria:

- MOH Audio Stream Number
- MOH Audio Source Name

Note To find all Music On Hold audio sources that are registered in the database, leave the text box blank and click **Find**.

Step 3 From the second drop-down list box, choose a search pattern for your search; for example, begins with, contains, or ends with.

Step 4 Specify the appropriate search text, if applicable, and click **Find**.

The records that match your search criteria display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Tip To search for MOH audio sources within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.

Note You can delete multiple Music On Hold audio sources from the Find and List Music On Hold Audio Sources window by checking the check boxes next to the appropriate Music On Hold audio sources and clicking **Delete Selected**. You can choose all of the Music On Hold audio sources in the window by clicking **Select All**.

Note that deletion does not remove the Music On Hold audio source files. Deletion only removes the association with the MOH Audio Stream number.

Step 5 From the list of records that match your search criteria, click the name of the Music On Hold audio source that you want to view.

The Music On Hold Audio Source Configuration window displays with the Music On Hold audio source that you choose.

Additional Information

See the "Related Topics" section on page 6-28.

Configuring a Music On Hold Audio Source

Perform the following procedure to add or update a Music On Hold audio source. Use this procedure to associate an existing audio source with an audio stream number or to upload a new custom audio source.

Note If a new version of an audio source file is available, you must perform the update procedure to use the new version.

Procedure

Step 1 Choose **Media Resources > Music On Hold Audio Source**.

The Find and List Music On Hold Audio Sources window displays.

Step 2 Perform one of the following tasks:

- To add a new Music On Hold audio source, click **Add New**.

  The Music On Hold Audio Source Configuration window displays.
- To update a Music On Hold audio source, locate a specific Music On Hold audio source as described in "Finding a Music On Hold Audio Source" section on page 6-17

Step 3 Enter the appropriate settings as described in Table 6-5.

Step 4 Click **Save**.

If you added a Music On Hold Audio Source, the list box at the bottom of the window now includes the new Music On Hold audio source.

Note The MOH Audio Source File Status pane tells you about the MOH audio translation status for the added source.

Additional Information

See the "Related Topics" section on page 6-28.

Deleting a Music On Hold Audio Source

Perform the following procedure to delete an existing Music On Hold audio source.

Note Deletion does not remove the Music On Hold audio source files. Deletion only removes the association with the MOH Audio Stream number.

Procedure

Step 1 Choose **Media Resources > Music On Hold Audio Source**.

The Find and List Music On Hold Audio Sources window displays.

Step 2 To locate a specific Music On Hold audio source, enter search criteria and click **Find**.

A list of Music On Hold audio sources that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the Music On Hold audio sources that you want to delete and click **Delete Selected**.
- Delete all Music On Hold audio sources in the window by clicking **Select All** and then clicking **Delete Selected**.
- From the list, choose the name of the Music On Hold audio source that you want to delete and click **Delete**.

A confirmation dialog displays.

Step 4 Click **OK**.

The association of the chosen Music On Hold audio source with an audio stream number gets deleted.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Audio Source Configuration Settings

Table 6-5 describes the configuration settings that are used for configuring Music On Hold audio sources.

Table 6-5 Music On Hold Audio Source Configuration Settings

Field	Description
Music On Hold Audio Source Information	
MOH Audio Stream Number	Use this field to choose the stream number for this MOH audio source. To do so, click the drop-down arrow and choose a value from the list that displays. For existing MOH audio sources, this value displays in the MOH Audio Source title.
MOH Audio Source File	Use this field to choose the file for this MOH audio source. To do so, click the drop-down arrow and choose a value from the list that displays.
Upload File	To upload an MOH audio source file that does not display in the drop-down list box, click the **Upload File** button. In the Upload File popup window that displays, enter the path to a file that specifies an audio source file. If you do not know the path and file name, search for the file by clicking the **Browse...** button to the right of the File field. After you locate the audio source file, click the **Upload** button to complete the upload. After the audio file gets uploaded, the Upload Result window tells you the result of the upload. Click **Close** to close this window. **Note** Uploading a file uploads the file to the Cisco CallManager server and performs audio conversions to create codec-specific audio files for MOH. Depending on the size of the original file, processing may take several minutes to complete. **Note** Uploading an audio source file to an MOH server uploads the file only to one MOH server. You must upload an audio source file to each MOH server in a cluster by using Cisco CallManager Administration on each server. MOH audio source files do *not* automatically propagate to other MOH servers in a cluster.
MOH Audio Source Name	Enter a unique name in this field for the MOH audio source. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Play continuously (repeat)	To specify continuous play of this MOH audio source, check this check box. **Note** Cisco recommends checking this check box. If continuous play of an audio source is not specified, only the first party placed on hold, not additional parties, will receive the MOH audio source.
Allow Multicasting	To specify that this MOH audio source allows multicasting, check this check box.

Table 6-5 Music On Hold Audio Source Configuration Settings (continued)

Field	Description
MOH Audio Source File Status	This pane displays information about the source file for a chosen MOH audio source. For an MOH audio source, the following attributes display: • Input File Name • Error Code • Error Text • Duration (in) Seconds • Disk Space KB • Low Date Time • High Date Time • Output File List – ULAW wav file name and status – ALAW wav file name and status – G.729 wav file name and status – Wideband wav file name and status • Date MOH Audio Translation completed
MOH Server Reset Information	To reset all MOH servers, click the **Reset** button. **Note** Cisco CallManager makes Music On Hold unavailable while the servers reset.
MOH Audio Sources	
(list of MOH audio sources)	For each MOH audio source that has been added, the MOH audio source name displays in this list box. Click the name of an MOH audio source to configure that MOH audio source.

Additional Information

See the "Related Topics" section on page 6-28.

Fixed Music On Hold Audio Source Configuration

The Music On Hold server supports one fixed-device stream source in addition to the file stream sources. This source represents the fixed audio source, which gets configured in the Fixed Music On Hold (MOH) Audio Source Configuration window. The fixed audio source gets sourced from a fixed device that uses the local computer audio driver.

For each cluster, you may define one fixed audio source. You must set up the fixed audio source that is configured per cluster on each MOH server. To do so, use the Cisco USB MOH sound adaptor, which must be ordered separately.

Use the following topics to configure the fixed Music On Hold audio source:

- Configuring the Fixed Music On Hold (MOH) Audio Source, page 6-22
- Deleting a Fixed Music On Hold (MOH) Audio Source, page 6-22
- Fixed Music On Hold (MOH) Audio Source Configuration Settings, page 6-23

Configuring the Fixed Music On Hold (MOH) Audio Source

Perform the following procedure to configure the fixed Music On Hold audio source.

Procedure

Step 1 Choose **Media Resources > Fixed MOH Audio Source**.

The Fixed MOH Audio Source Configuration window displays.

Step 2 To configure and enable a fixed Music On Hold (MOH) audio source, enter the appropriate settings as described in Table 6-6.

Step 3 Click **Save**.

The Fixed MOH Audio Source Configuration window displays an *Update Successful* status message.

Additional Information

See the "Related Topics" section on page 6-28.

Deleting a Fixed Music On Hold (MOH) Audio Source

Perform the following procedure to delete an existing fixed Music On Hold audio source.

Procedure

Step 1 Choose **Media Resources > Fixed MOH Audio Source**.

The Fixed MOH Audio Source Configuration window displays.

Step 2 If the fixed MOH audio source that displays is enabled (that is, the Enable check box has been checked), you can delete this fixed MOH audio source.

To delete this fixed MOH audio source, click **Delete**.

A confirmation dialog box displays.

Step 3 Click **OK**.

The chosen fixed Music On Hold audio source gets deleted from the database.

Additional Information

See the "Related Topics" section on page 6-28.

Fixed Music On Hold (MOH) Audio Source Configuration Settings

Table 6-6 describes the configuration settings that are used for configuring the fixed Music On Hold (MOH) audio source.

Table 6-6 Fixed Music On Hold (MOH) Audio Source Configuration Settings

Field	Description
Fixed MOH Audio Source Information	
Source ID	This field displays the stream number for this fixed MOH audio source.
Name	Enter a unique name in this field for the fixed MOH audio source. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Allow Multicasting	To specify that this fixed MOH audio source allows multicasting, check this check box.
Enable (If checked, Name is required.)	To enable this fixed MOH audio source, check this check box.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Server Configuration

You can configure servers for Music On Hold for a media resource group. Use the following topics to configure Music On Hold servers:

- Finding a Music On Hold Server, page 6-23
- Configuring a Music On Hold Server, page 6-24
- Resetting or Restarting a Music On Hold Server, page 6-25
- Music On Hold Server Configuration Settings, page 6-26

For any Music On Hold server that you configure, you may trace the configuration of that server. Refer to the *Cisco CallManager Serviceability Administration Guide* and *the Cisco CallManager Serviceability System Guide* for more information.

Additional Information

See the "Related Topics" section on page 6-28.

Finding a Music On Hold Server

Because you might have several music on hold servers in your network, Cisco CallManager lets you locate specific music on hold servers on the basis of specific criteria. Use the following procedure to locate music on hold servers.

Procedure

Step 1 Choose **Media Resources > Music On Hold Server**.

The Find and List Music On Hold Servers window displays. Use the two drop-down list boxes to search for a music on hold server.

Step 2 From the first Find Music On Hold Servers where drop-down list box, choose one of the following criteria:

- Name
- Description
- Device Pool Name

Tip To find all music on hold servers that are registered in the database, click **Find** without entering any search text.

Step 3 From the second Find Music On Hold Servers where drop-down list box, choose a search pattern for your text search; for example, begins with, contains, or ends with.

Step 4 Specify the appropriate search text, if applicable, and click **Find**.

The records that match your search criteria display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Tip To search for Music On Hold servers within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.

Step 5 From the list of records that match your search criteria, click the name of the Music On Hold server that you want to view.

The Music On Hold (MOH) Server Configuration window displays with the Music On Hold server that you choose.

Additional Information

See the "Related Topics" section on page 6-28.

Configuring a Music On Hold Server

Perform the following procedure to update a Music On Hold server.

Note You cannot add nor delete a Music On Hold server.

Procedure

Step 1 Choose **Media Resources > Music On Hold Server**.

The Find and List Music On Hold Servers window displays. Use the two drop-down list boxes to search for a music on hold server.

Step 2 Perform one of the following tasks:

- To update a Music On Hold server, click the Music On Hold server that you want to update

  The Music On Hold (MOH) Server Configuration window displays.

Step 3 Enter or update the appropriate settings as described in Table 6-7.

Step 4 To update this Music On Hold server, click **Save**.

The Music On Hold server gets updated in the database.

Additional Information

See the "Related Topics" section on page 6-28.

Resetting or Restarting a Music On Hold Server

Perform the following procedure to reset an existing Music On Hold server.

Procedure

Step 1 Locate the music on hold server by using the procedure in the "Finding a Music On Hold Server" section on page 6-23.

Step 2 Click the music on hold server that you want to reset.

Step 3 Click the **Reset** button.

A popup window displays an information message.

Step 4 After reading the message, click **Restart** to restart the music on hold server or click **Reset** to reset the music on hold server.

Step 5 To close the popup window, click **Close**.

Additional Information

See the "Related Topics" section on page 6-28.

Music On Hold Server Configuration Settings

Table 6-7 describes the configuration settings that are used for configuring Music On Hold servers.

Table 6-7 Music On Hold Server Configuration Settings

Field	Description
Device Information	
Host Server	For existing Music On Hold servers, this field is display only.
Music On Hold Server Name	Enter a unique name for the Music On Hold server in this required field. This name can comprise up to 15 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Description	Enter a description for the Music On Hold server. This description can comprise up to 50 characters. Ensure Description does not contain ampersand (&), double quotes ("), brackets ([]), less than (<), greater than (>), or the percent sign (%).
Device Pool	Use this required field to choose a device pool for the Music On Hold server. To do so, click the drop-down arrow and choose a device pool from the list that displays.
Location	Choose the appropriate location for this MOH server. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of *None* means that the locations feature does not keep track of the bandwidth that this MOH server consumes.
Maximum Half Duplex Streams	Enter a number in this required field for the maximum number of half-duplex streams that this Music On Hold server supports. Valid values range from 0 to 500.
Maximum Multicast Connections	Enter a number in this required field for the maximum number of multicast connections that this Music On Hold server supports. Valid values range from 1 to 999999.
Fixed Audio Source Device	Enter the device name of the fixed audio source device. This device serves as the per-server override that is used if the server has a special sound device installed.
Run Flag	Use this required field to choose a run flag for the Music On Hold server. To do so, click the drop-down arrow and choose **Yes** or **No**. Choosing **No** disables the Music On Hold server.
Multicast Audio Source Information	
Enable Multicast Audio Sources on this MOH Server	Check or uncheck this check box to enable or disable multicast of audio sources for this Music On Hold server. **Note** If this MOH server belongs to a multicast media resource group, a message asks you to enable multicast on this MOH server or to update the specified media resource group(s) either by removing this MOH server or by changing the multicast setting of each group listed.

Table 6-7 Music On Hold Server Configuration Settings (continued)

Field	Description
Base Multicast IP Address	If multicast support is needed, enter the base multicast IP address in this field. Valid IP addresses for multicast range from 224.0.1.0 to 239.255.255.255. **Note** IP addresses between 224.0.1.0 and 238.255.255.255 fall in the reserved range of IP multicast addresses for public multicast applications. Use of such addresses may interfere with existing multicast applications on the Internet. Cisco strongly recommends using IP addresses in the range that is reserved for administratively controlled applications on private networks (239.0.0.0 - 239.255.255.255).
Base Multicast Port Number	If multicast support is needed, enter the base multicast port number in this field. Valid multicast port numbers include even numbers that range from 16384 to 32766.
Increment Multicast on	Click **Port Number** to increment multicast on port number. Click **IP Address** to increment multicast on IP address. **Note** Multicast by incrementing IP address is preferable in firewall situations. This results in each multicast audio source having a unique IP address and helps to avoid network saturation.
Selected Multicast Audio Sources	
	Only audio sources for which the Allow Multicasting check box was checked display in this listing. If no such audio sources exist, the following message displays: There are no Music On Hold Audio Sources selected for Multicasting. Click Configure Audio Sources in the top right corner of the page to select Multicast Audio Sources. From the Related Links drop-down list box, choose Configure Audio Sources and click **Go**.
No.	This field designates Music On Hold audio stream number that is associated with a particular multicast audio source. Only audio sources that are defined as allowing multicasting display.
Audio Source Name	This field designates name of audio source that is defined as allowing multicasting.
Max Hops	For each multicast audio source, enter the maximum number of router hops through which multicast packets should pass. Valid values range from 1 to 15. **Note** Using high values can lead to network saturation. This field is also known as *Time to Live*.

Additional Information

See the "Related Topics" section on page 6-28.

Related Topics

- Understanding Music On Hold, page 6-1
- Music On Hold Definitions, page 6-2
- Music On Hold Characteristics, page 6-3
- Music On Hold Functionality, page 6-4
- Supported Music On Hold Features, page 6-5
- Music On Hold System Requirements and Limits, page 6-12
- Music On Hold Failover and Fallback, page 6-13
- Music On Hold Configuration Checklist, page 6-14
- Monitoring Music On Hold Performance, page 6-15
- Viewing Music On Hold Server Performance, page 6-15
- Media Resource Group Configuration, *Cisco CallManager Administration Guide*
- Media Resource Group List Configuration, *Cisco CallManager Administration Guide*

Music On Hold Audio Sources

- Music On Hold Audio Sources, page 6-8
- Storing Audio Source Files, page 6-9
- Finding a Music On Hold Audio Source, page 6-17
- Configuring a Music On Hold Audio Source, page 6-18
- Deleting a Music On Hold Audio Source, page 6-19
- Music On Hold Audio Source Configuration Settings, page 6-19

Fixed Music On Hold Audio Source

- Fixed Music On Hold Audio Source Configuration, page 6-21
- Configuring the Fixed Music On Hold (MOH) Audio Source, page 6-22
- Deleting a Fixed Music On Hold (MOH) Audio Source, page 6-22
- Fixed Music On Hold (MOH) Audio Source Configuration Settings, page 6-23

Music On Hold Servers

- Music On Hold Server, page 6-8
- Music On Hold Server Configuration, page 6-23
- Finding a Music On Hold Server, page 6-23
- Configuring a Music On Hold Server, page 6-24
- Resetting or Restarting a Music On Hold Server, page 6-25
- Music On Hold Server Configuration Settings, page 6-26

Additional Cisco Documentation

- *Installing Cisco CallManager Release 5.0(1)*
- *Upgrading Cisco CallManager Release 5.0(1)*

- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*

Cisco CallManager AutoAttendant

Cisco CallManager AutoAttendant, a simple automated attendant, allows callers to locate people in your organization without talking to a receptionist. You can customize the prompts that are played for the caller, but you cannot customize how the software interacts with the customer.

Cisco CallManager AutoAttendant comes bundled with Cisco CallManager on the Cisco CallManager 5 agent IPCC Express bundle.

This chapter describes Cisco CallManager AutoAttendant that is running on Cisco CRS 4.5.

Note For information about supported versions of Cisco CRS with Cisco CallManager, see the Cisco CallManager Compatibility Matrix at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm#CompatibleApplications

Use the following topics to understand, install, configure, and manage Cisco CallManager AutoAttendant:

- Understanding Cisco CallManager AutoAttendant, page 7-1
- Installing and Upgrading the Customer Response Solutions (CRS) Engine, page 7-3
- Configuring Cisco CallManager AutoAttendant and the CRS Engine, page 7-4
- Managing Cisco CallManager AutoAttendant, page 7-24

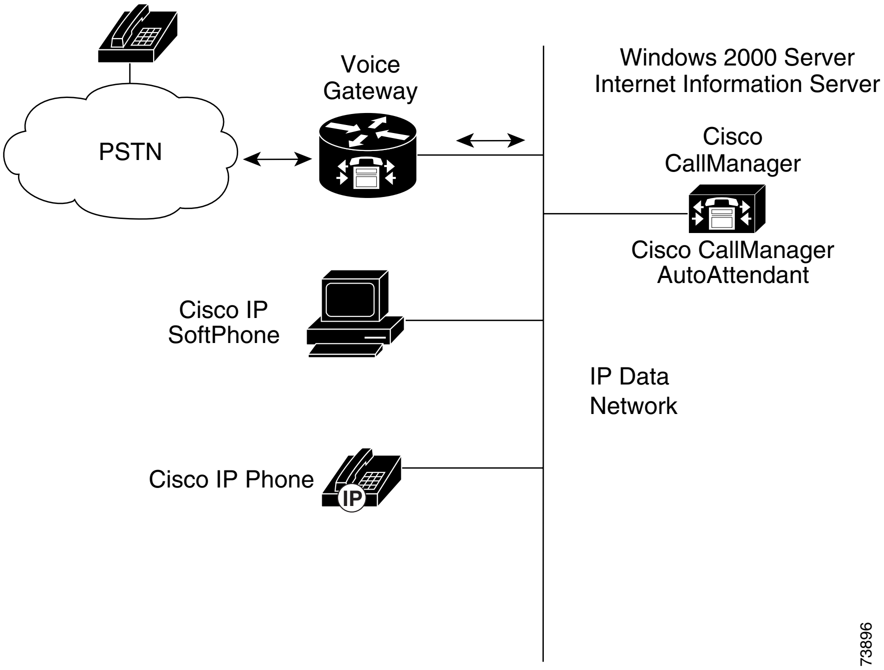
Understanding Cisco CallManager AutoAttendant

Cisco CallManager AutoAttendant (see Figure 7-1) works with Cisco CallManager to receive calls on specific telephone extensions. The software interacts with the caller and allows the caller to search for and select the extension of the party (in your organization) that the caller is trying to reach.

This section provides an introduction to Cisco CallManager AutoAttendant:

- Cisco CallManager AutoAttendant Overview, page 7-2
- Components of Cisco CallManager AutoAttendant, page 7-3

Figure 7-1 Using Cisco CallManager AutoAttendant



Cisco CallManager AutoAttendant Overview

Cisco CallManager AutoAttendant provides the following script:

- Answers a call
- Plays a user-configurable welcome prompt
- Plays a main menu prompt that asks the caller to perform one of three actions:
  - Press 0 for the operator.
  - Press 1 to enter an extension number.
  - Press 2 to spell by name.
- If the caller chooses to spell by name (by pressing 2), the system compares the letters that are entered with the names that are configured to the available extensions.
  - If a match exists, the system announces a transfer to the matched user and waits for up to 2 seconds for the caller to press any DTMF key to stop the transfer. If the caller does not stop the transfer, the system performs an explicit confirmation: it prompts the user for confirmation of the name and transfers the call to that user's primary extension.
  - If more than one match occurs, the system prompts the caller to choose the correct extension.
  - If too many matches occur, the system prompts the caller to enter more characters.
- When the caller has specified the destination, the system transfers the call.
  - If the line is busy or not in service, the system informs the caller accordingly and replays the main menu prompt.

Additional Information

See the "Related Topics" section on page 7-24

Components of Cisco CallManager AutoAttendant

The Cisco Customer Response Solutions Platform provides the components that are required to run Cisco CallManager AutoAttendant. The platform provides a multimedia (voice/data/web) IP-enabled customer care application environment.

Note Cisco Customer Response Solutions (CRS) gets marketed under the names IPCC Express and IP IVR which are products on the Cisco CRS platform.

Cisco CallManager AutoAttendant uses three main components of the Cisco Customer Response Solutions Platform:

- Gateway—Connects the enterprise IP telephony network to the Public Switched Telephone Network (PSTN) and to other private telephone systems such as Public Branch Exchange (PBX). You must purchase gateways separately.
- Cisco CallManager Server—Provides the features that are required to implement IP phones, manage gateways, provides failover and redundancy service for the telephony system, and directs voice over IP traffic to the Cisco Customer Response Solutions (Cisco CRS) system. You must purchase Cisco CallManager separately.
- Cisco CRS Server—Contains the Cisco CRS Engine that runs Cisco CallManager AutoAttendant. The Cisco CallManager AutoAttendant package includes the Cisco CRS Server and Engine.

For more information about the Cisco Customer Response Solutions Platform, refer to the following URL.

http://www.cisco.com/en/US/products/ps5883/index.html

Additional Information

See the "Related Topics" section on page 7-24

Installing and Upgrading the Customer Response Solutions (CRS) Engine

Use these topics to install or upgrade CRS:

- Hardware and Software Requirements, page 7-3.
- Installing or Upgrading Cisco CallManager AutoAttendant, page 7-4.

Hardware and Software Requirements

Before you install this version of CRS, you must have a functioning voice over IP system. You must have installed and configured Cisco CallManager 5.0. This software manages the telephony system.

Cisco CallManager AutoAttendant runs on the Cisco Media Convergence Server (Cisco MCS) platform or on a Cisco-certified server.

Ensure that the Cisco CallManager server is running on an appliance based system.

Installing or Upgrading Cisco CallManager AutoAttendant

Install Cisco CallManager on an appliance based system before you install
Cisco CallManager AutoAttendant on the CRS server. For information, refer to the following documents:

- Cisco CallManager installation documentation at

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/install/instcall/index.htm
- Cisco IP Telephony Operating System at

  http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm

You must configure proxy settings for Internet Explorer and verify that you can browse to internal and external web sites. For details on configuring your proxy settings, contact your network administrator.

Before You Begin

Ensure that you have met all preinstallation requirements that are described in Hardware and Software Requirements, page 7-3

This topic describes how to install Cisco CallManager AutoAttendant:

- Installing Cisco CallManager AutoAttendant, page 7-4.

Installing Cisco CallManager AutoAttendant

The following procedure describes how to install Cisco CallManager IPCC Express 5 Seat Bundle for the first time. Complete the following steps only once after a fresh install.

Procedure 1

Step 1 Download the Cisco CallManager AutoAttendant software package from CCO to an MCS server.

Step 2 To start the installation program, click the .exe file and follow the on-screen instructions.

Additional Information

See the "Related Topics" section on page 7-24

Configuring Cisco CallManager AutoAttendant and the CRS Engine

These topics describe how to configure Cisco CallManager and the Cisco Customer Response Solutions (CRS) Engine in preparation for deploying Cisco CallManager AutoAttendant.

Configuration Checklist for Cisco CallManager AutoAttendant

Table 7-1 describes the procedures that you perform to configure Cisco CallManager AutoAttendant.

Table 7-1 Configuration Checklist for Cisco CallManager AutoAttendant

Configuration Steps		Related Procedures and Topics
Step 1	Configure the Cisco Customer Response Solutions (CRS) Engine. You must install and configure Cisco CRS before you can use Cisco CallManager AutoAttendant. The Cisco CRS Engine controls the software and its connection to the telephony system	See "Configuring the Cisco Customer Response Solutions Engine" section on page 7-9. See also *Cisco CRS Installation Guide*.
Step 2	Customize Cisco CallManager AutoAttendant, so its prompts are meaningful to the way that you are using the automated attendant.	See the "Customizing Cisco CallManager AutoAttendant" section on page 7-20.

Configuring Cisco CallManager

Before you can use Cisco CallManager AutoAttendant, you must configure Cisco CallManager.

These topics assume that you know how to use Cisco CallManager. For more information about Cisco CallManager, refer to the *Cisco CallManager Administration Guide* and the *Cisco CallManager System Guide*.

Configuring a Cisco CallManager User for Cisco CallManager AutoAttendant

Create user to log in as a CRS administrator on the AutoAttendant.

Procedure

Step 1 In Cisco CallManager, choose **User Management>End User**.

Step 2 Cisco CallManager opens the Find and List Users window. Click **Add New**.

The End User Configuration window displays. Complete the fields as described in Table 7-2.

Step 3 To create the user, click **Save**.

Cisco CallManager adds the user.

Table 7-2 Configuring a Cisco CallManager User for Cisco CallManager AutoAttendant

Field	Description
LDAP Sync Status	This field displays the LDAP synchronization status, which is set with the System > LDAP > LDAP System menu option.
User ID	Enter the end user identification name. Cisco CallManager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
Password	Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
Confirm Password	Enter the user password again.
PIN	Enter five or more numeric characters for the Personal Identification Number.
Confirm PIN	Enter the PIN again.
Last Name	Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
Middle Name	Enter the end user middle name. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
First Name	Enter the end user first name. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
Telephone Number	Enter the end user telephone number. You may use the following special characters: (,) and - .
Mail ID	This description will be provided in Release 5.0(1) of Cisco CallManager Administration.
Manager User ID	Enter the name of the end user manager ID. The manager user ID that you enter must already exist in the directory as an end user.
Department	Enter the end user department information (for example, the department number or name).

Table 7-2 Configuring a Cisco CallManager User for Cisco CallManager AutoAttendant (continued)

Field	Description
User Locale	From the drop-down list box, choose the locale that is associated with the end user. The user locale identifies a set of detailed information to support end users, including language and font. Cisco CallManager uses this locale for extension mobility and the Cisco IP Phone User Options. For Cisco CallManager Extension Mobility log on, the locale that is specified here takes precedence over the device and device profile settings. For Cisco CallManager Extension Mobility log off, Cisco CallManager uses the end user locale that the default device profile specifies. **Note** If you do not choose an end user locale, the locale that is specified in the Cisco CallManager service parameters as Default User Locale applies.
Associated PC	Use this required field for Cisco SoftPhone and Cisco CallManager Attendant Console users.
Digest Credentials	When you configure digest authentication for SIP phones, Cisco CallManager challenges the identity of the phone every time that the phone sends a SIP request to Cisco CallManager. The digest credentials that you enter in this field get associated with the phone when you choose a digest user in the Phone Configuration window. Enter a string of alphanumeric characters. **Note** For more information on digest authentication, refer to the *Cisco CallManager Security Guide*.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.

Table 7-2 Configuring a Cisco CallManager User for Cisco CallManager AutoAttendant (continued)

Field	Description
Device Associations	
Available Devices	This list box displays the devices that are available for association with this end user. To associate a device with this end user, select the device and click the Down Arrow below this list box. If the device that you want to associate with this end user does not display in this pane, click one of these buttons to search for other devices: • **Find more Phones**-Click this button to find more phones to associate with this end user. The Find and List Phones window displays to enable a phone search • **Find more Route Points**-Click this button to find more route points to associate with this end user. The Find and List CTI Route Points window displays to enable a CTI route point search.
Controlled Devices	After the device is associated, this field displays the description information (for example, the MAC address) that the end user controls.
Extension Mobility	
Available Profiles	This list box displays the extension mobility profiles that are available for association with this end user. To associate an extension mobility profile with this end user, select the profile and click the Down Arrow below this list box.
Controlled Profiles	This field displays a list of controlled device profiles that are associated with an end user who is configured for Cisco CallManager Extension Mobility.
Default Profile	From the drop-down list box, choose a default extension mobility profile for this end user.
Presence Group	From the drop-down list box, choose the presence group that watches the status of the directory number, the presence entity.

Table 7-2 Configuring a Cisco CallManager User for Cisco CallManager AutoAttendant (continued)

Field	Description
SUBSCRIBE Calling Search Space	All calling search spaces that you configure in Cisco CallManager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. The SUBSCRIBE Calling Search Space determines how Cisco CallManager routes the Presence subscription requests that come from the end user. To configure a calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces (Call Routing > Class Control > Calling Search Space).
Allow Control of Device from CTI	The system checks this box by default. Leave it checked if you want to allow control of the device from the CTI.
Directory Number Associations	
Primary Extension	This field represents the primary directory number for the end user. You choose no primary line when you associate devices to the end user. End users can have multiple lines on their phones. From the drop-down list box, choose a primary extension for this end user. If the system is configured for Unity Integration, the Create Voice Mailbox link displays.

Additional Information

See the "Related Topics" section on page 7-24

Configuring the Cisco Customer Response Solutions Engine

Configure the Cisco Customer Response Solutions (CRS) Engine to communicate with Cisco CallManager and the Cisco IP Telephony Directory. Perform the configuration steps that are shown in the following sections:

- Cluster Setup, page 7-10
- Server Setup, page 7-11
- Adding a JTAPI Call Control Group, page 7-11
- Provisioning Cisco Media Termination Subsystem, page 7-15
- Adding a New Cisco CallManager AutoAttendant, page 7-16
- Configuring a JTAPI Trigger, page 7-17
- Modifying an Instance of Cisco CallManager AutoAttendant, page 7-20

These topics only cover the basics of using and configuring Cisco CRS. See the Cisco CRS online help for more detailed information.

Additional Information

See the "Related Topics" section on page 7-24

Tip To start Cisco CRS Administration, open http://*servername*/AppAdmin in your web browser, where *servername* specifies the DNS name or IP address of the application server. Click Help for detailed information about using the interface.

Cluster Setup

Perform the following steps to set up the cluster.

Step 1 Log in to the CRS server by using **Administrator** as the UserID and **ciscocisco** as the password.

Step 2 The Cisco CRS Administrator Setup window displays. Click **Setup**.

Step 3 The License Information window displays. Click **Browse** to locate the free IPCC Express license that you downloaded from CCO. Highlight the license and click **Next**. The same window may appear again if so, click **Next**.

Step 4 The CallManager Configuration window displays.

- Under AXL Service Provider Configuration, you will see the available AXL Service Providers in the field on the right. Select your service provider and click the triangular shaped button that points toward the left. The selected AXL Service Provider appears under Selected AXL Service Providers.

  In the User Name and Password fields, enter the username and password that you used to access information through AXL on the Cisco CallManager side.

- Under JTAPI Subsystem - JTAPI Provider Configuration, in the Available CTI Managers, select the appropriate CTI Manager and click the triangular shaped button that points toward the left. The selected CTI Manager appears under Selected CTI Managers.

  In the User Prefix and Password fields, create a User Prefix and Password.

Note Do nothing in the RmCm Subsystem section of the CallManager Configuration window.

- Click **Next**.

Step 5 The User Management window displays. The Cisco CallManager users appear in the CMUsers field. Select the user that was created on the Cisco CallManager, see Configuring a Cisco CallManager User for Cisco CallManager AutoAttendant, page 7-5

- Click the triangular shaped button that points toward the left. The selected user appears in the CRS Administrator / Supervisor field.

Note If you click **Search**, the system will search the Cisco CallManager side for users.

- Click **Next**.

Step 6 The Directory Setup window displays. Close your browser.

You have completed cluster setup.

Note After you set up the username and password in cluster setup, you will need to use that username and password for Server Setup.

Server Setup

Now that you have completed the cluster setup, you must set up the server.

Step 1 From the CRS server, click **Start >Programs >Administrator Tools >Services**.

Step 2 In the window that displays, highlight the Cisco CRS Node Manager and click the **Restart Service** button at the top of the window.

Step 3 Launch CRS Administration.

Step 4 Log in to the CRS server by using the user name that you chose on the User Management window in Cluster Setup, page 7-10.

Step 5 The Cisco CRS Administrator Setup window displays. Click **Setup**.

Step 6 The Component Activation window displays. Check the check boxes next to CRS Agent Datastore, CRS Config Datastore, CRS Engine, CRS Historical Datastore, CRS Node Manager, and CRS Repository Datastore and click **Next.**

Step 7 The Publisher Activation window displays. Choose your CRS server for each Datastore and click **Activate Publisher**.

Step 8 The Server Setup window displays and shows that server setup is complete.

Note Do update the HR session license as shown on the Server Setup window if you are using the CRS Historical Reporting Client.

Note Now that the server has been setup, you will need to use the new username and password that you created.

Additional Information

See the "Related Topics" section on page 7-24

Adding a JTAPI Call Control Group

Perform the following steps to add a JTAPI call control group.

Step 1 Go to **Subsystems > JTAPI**. The JTAPI Call Control Configuration window displays.

Step 2 Click **Add a New JTAPI Call Control Group**. Enter the required information as shown in Table 7-3.

Step 3 Click **Add**.

Table 7-3 Configuring a JTAPI Call Control Group

Field	Description
Group Information	
Group ID	This field corresponds to the trunk group number that was reported to Cisco ICM when the CRS server is part of the Cisco ICM/IPCC Enterprise solution. Accept the automatic Group ID or enter a unique description.
Description	Press the Tab key to automatically populate the description field.
Number of CTI Ports	Enter the number of CTI ports that are assigned to the group. **Note** If this field is set to <*n*>, the system will create <*n*> ports for each CRS engine node (node in which CRS engine component is enabled).
Directory Number	
Starting Directory Number	This field specifies a unique phone number. The value can include numeric characters and special characters # and *. The specified number of ports get created starting from the value that is specified in this field. The directory number that you enter can appear in more than one partition. **Note** When a pattern is used as a directory number, the phone display and the caller ID display on the dialed phone will contain characters of the digits. To avoid this situation, provide a value for Display (Internal Call ID), Line Text Label, and External Phone Number Mask.

Table 7-3 Configuring a JTAPI Call Control Group (continued)

Field	Description
Group Information	

Device Name Prefix	The system uses the device name prefix (DNP) in the name that will be given all the CTI ports in this group.
	The CTI ports for this port group will have the device name of the format:
	`<deviceprefix>_<directoryno>`
	`For example, if the device name prefix is CTIP and the starting directory number is 7000, the CTI port that is created in Cisco CallManager will have the device name CTIP_7000 and will use the line 7000.`
	Note The system restricts the device name prefix to 5 characters.

Device Pool	This field specifies the device pool (sets of common characteristics for devices such as region, date/time group, softkey template, and MLPP information) to which you want to assign this phone.
DN Calling Search Space	This field specifies a collection of partitions that are searched to determine how a dialed number should be routed, the calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS.
Redirect Calling Search Space	This field specifies a collection of partitions that are searched to determine how a redirected call should be routed.
Media Resource Group List	A prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On hold server, from the available media resources according to the propriety order that is defined in a Media Resource Group List. If you choose **None**, Cisco CallManager uses the Media Resource Group that is defined in the device pool.
Location	The Cisco IP Phone location setting specifies the total bandwidth that is available for calls to and from this location. A location setting of **None** means that the location feature does not keep track of the bandwidth that this Cisco IP Phone consumes.

Table 7-3 Configuring a JTAPI Call Control Group (continued)

Field	Description
Group Information	
Partition	This field specifies the partition to which the directory number belongs. The directory number field value is unique within the partition that you choose. If you do not want to restrict access to the directory number, select **None** as the partition setting.
Directory Number Setting	
Voice Mail Profile	From the drop-down list, choose **None**, **NoVoiceMail** or **Default**.
AAR Group	From the drop-down list, choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of **None** specifies that no rerouting of blocked calls will be attempted.
User Hold Audio Source	From the drop-down list, choose the audio source that will play when a user initiates a hold action.
Network Hold Audio Source	From the drop-down list, choose the audio source that will play when a user initiates a hold action.
Call Pickup Group	From the drop-down list, choose the number that can be dialed to answer calls to this directory number in the specified partition.
Display	Enter a maximum of 40 alphanumeric characters. Typically, use the user name or the directory number (if the directory number is used, the receiving phone may not show the proper identity of the caller). Leave this field blank to have the system display the extension.

External Phone Number Mask	Enter a maximum of 30 numbers and “X” characters to indicate the phone number (or mask) that is used to send Caller ID information when a call is placed from this line.
	The Xs represent the directory number and must appear at the end of the pattern.
	`For example:`
	`If you specify a mask of 972813XXXX, an internal call form extension 1234 displays a caller ID number of 9728131234.`

Provisioning Cisco Media Termination Subsystem

You can choose different types of media, from a simple type of media that is capable of supporting prompts and DTMF (Cisco Media Termination) to a more complex and rich type of media that is capable of supporting speech recognition in addition to prompts and DTMFs. You can even provision calls without media. Because of these capabilities, you must provision media manually. Each call requires both a CTI port and a media channel for the system to be backward compatible or to support media interactions.

Furthermore, because media resources are licensed and sold as IVR ports, you can provision more channels than you are licensed for and, at run-time, licensing will be enforced to prevent the system from accepting calls, as this would violate your licensing agreements.

You can provision Call Control groups, multiple CMT Dialog groups, and Nuance ASR Dialog groups to allow for the sharing of resources between different applications. In addition, you can provision special applications to primarily use specific sets of resources. You can do this, for example, when you configure a JTAPI Trigger. For more information, see the *Cisco Customer Response Solutions Administration Guide*.

Provisioning CMT Dialog Groups

The Cisco CRS server uses the Real-Time Transport Protocol (RTP) to send and receive media packets over the IP network. To ensure that the CRS Engine can communicate with your Cisco IP Telephony system, you need to configure the RTP ports that the CRS Engine will use to send and receive RTP data.

To configure a CMT Dialog, perform the following steps:

Procedure

Step 1 Connect to Cisco CRS Administration.

Step 2 From the CRS Administration main menu, choose **Subsystems > Cisco Media**.

The Cisco Media Termination Dialog Group Configuration window displays.

Step 3 Click the **Add a New CMT Dialog Group** hyperlink.

The second Cisco Media Termination Dialog Group Configuration window displays.

Step 4 Accept the automatic group ID or enter a group ID in the Group ID field.

Note Ensure this Group ID is unique within all media group identifiers, including ASR.

Step 5 To automatically populate the Description field, press the **Tab** key.

Step 6 Enter a maximum number of channels that are available for the group in the Maximum Number Of Channels field.

Step 7 Click **Add**.

The Cisco Media Termination Dialog Group Configuration window displays.

Adding a New Cisco CallManager AutoAttendant

After you have configured the JTAPI subsystem on the Cisco CRS Engine, you can use one of the sample scripts to create an application and start the Cisco CRS Engine. To add a new Cisco CallManager AutoAttendant, use this procedure.

Tip To start Cisco CRS Administration, open http://*servername*/AppAdmin in your web browser, where *servername* specifies the DNS name or IP address of the application server. Click Help for detailed information on using the interface.

Procedure

Step 1 From the CRS Administration main menu, choose **Applications > Application Management**.

Cisco CRS Administration opens Application Configuration window.

Step 2 Click the **Add New Application** link on the Application Configuration window.

The Add a New Application window displays.

Step 3 Click **Next**.

The Cisco Script Application window displays.

Step 4 In the Name field, enter the name of the application.

Step 5 To automatically populate the Description field, press the **Tab** key.

Step 6 In the ID field, enter a unique ID. The ID gets reported in Historical Reporting to identify this application.

Note The system automatically generates an ID; therefore, you can use the ID that the field contains or erase the value and enter a new one.

Step 7 In the Maximum Number of Sessions field, enter the maximum number of sessions that can be running this application simultaneously.

Note Depending on the Script and Default Script selection, the window may refresh and provide additional fields and drop-down menu options.

Step 8 From the Script drop-down arrow, choose the script that will be running the application. The script for Cisco CallManager AutoAttendant specifies aa.aef.

Step 9 From the Default Script drop-down menu, accept **System Default**. The default script executes when an error occurs with the configured application script.

Step 10 Click **Add**.

The following message displays:

"The operation has been executed successfully"

Step 11 To close the dialog box, click **OK**.

Additional Information

See the "Related Topics" section on page 7-24

Configuring a JTAPI Trigger

Perform the following steps to configure a JTAPI trigger.

Step 1 Choose **Subsystems > JTAPI**. The JTAPI Call Control Group Configuration window displays.

Step 2 In the left column, click **JTAPI Triggers**. The JTAPI Trigger Configuration window displays.

Step 3 Click the **Add a New JTAPI Trigger** link. The second JTAPI Trigger Configuration window displays.

Step 4 Enter the required information as shown in Table 7-4.

Step 5 Click **Add**.

Step 6 Choose **Systems > Control Center**, check CRS Engine - JTAPI to ensure it is running. If it is not, click radio button and click restart.

Table 7-4 Configuring a JTAPI Trigger

Field	Description
Directory Number	

Directory Number	Enter a unique telephone number. The value includes numeric characters, preceded or appended by special characters (# or *).
	`Examples of valid directory numbers:`
	`##*1100**`
	`*#12#*`
	
	`Example of an invalid directory number:`
	`*12*23#`

Partition	Enter the partition of the directory to which the directory number belongs. Ensure the directory number field value is unique within the chosen partition. If you do not want to restrict access to the directory number, select **None** as the partition setting.
Trigger Information	
Language	From the drop-down list choose the preferred language. If your preferred language does not appear in the drop-down box, click **Edit**. • The Employer User Prompt dialog box opens. Enter a locale string value. • Click **OK**. The locale string value now will appear in the drop-down list. • Choose the preferred language.

Table 7-4 Configuring a JTAPI Trigger (continued)

Field	Description
Directory Number	
Application Name	From the drop-down list, choose the application to associate with the trigger.
Maximum Number of Sessions	Enter the maximum number of simultaneous calls that this trigger can handle.
Idle Timeout (in ms)	Enter the number of milliseconds that the system should wait before rejecting the JTAPI request for this trigger.
Enabled	To enable the trigger, choose **Yes**. To disable the trigger, choose **No**.
Call Control Group	From the drop-down list, choose the call control group to associate with the trigger.
Primary Dialog Group	From the drop-down list, choose the dialog group to associate with the trigger (if media is required by the associated application).
Secondary Dialog Group	From the drop-down list, choose a backup dialog group to associate with the trigger if the primary dialog group does not have enough resources to provide for an incoming call on this trigger.
CTI Route Point Information	
Device Name	Enter a unique identifier for this device, consisting of alphanumeric characters, dots, dashes, or underscores.
Description	Enter a descriptive name for the CTI route point.
Device Pool	From the drop-down list choose the device pool to which you want to assign this route point. A device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.
Location	From the drop-down list choose 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 route point uses.
Directory Number Settings	
Voice Mail Profile	From the drop-down list of voice mail profiles that are configured in the Voice Mail Profile configuration, choose the profile to which you want to associate this directory number. The default specifies **None**.

Table 7-4 Configuring a JTAPI Trigger (continued)

Field	Description
Directory Number	
Calling Search Space	From the drop-down list of partitions that are searched for numbers that are called from this directory number, choose the value to apply to all devices that use this directory number.
Call Forward and Pickup Settings	
Forward Busy	You have several options: • Voice Mail - Check this check box to use settings in the Voice Mail Profile Configuration. **Note** When this check box is checked, Cisco CallManager ignores the setting in the Destination box and Calling Search Space. • Destination - Enter the destination to which the call should be forwarded. • Calling Search Space - From the drop-down list, choose the calling search space to which the call should be forwarded.
Call Pickup Group	From the drop-down list, choose a number that can be dialed to answer calls to this directory number (in the specified partition).
Display	Leave this field blank to have the system display the extension of the caller. Or, enter a maximum of 30 alphanumeric characters. Typically, use the user name or the directory number (if using the directory number, the person receiving the call may not see the proper identity of the caller.).
External Phone Number Mask	Enter the phone number (or mask) that is used to send Caller ID information when a call is placed from this line You can enter a maximum of 30 numbers and “X” characters. The Xs represent the directory number and must appear at the end of the pattern. `For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234.`

Customizing Cisco CallManager AutoAttendant

Cisco CallManager AutoAttendant comes with a prerecorded welcome prompt. By default, it spells out user names; it does not attempt to pronounce names. You can customize your automated attendant by adding your own welcome prompt and recordings of your user spoken names. These topics describe how to customize Cisco CallManager AutoAttendant:

- Modifying an Instance of Cisco CallManager AutoAttendant, page 7-20
- Configuring Prompts, page 7-21

Modifying an Instance of Cisco CallManager AutoAttendant

This section describes how to modify Cisco CallManager AutoAttendant settings.

Tip To start Cisco CRS Administration, open http://*servername*/AppAdmin in your web browser, where *servername* specifies the DNS name or IP address of the application server. Click Help for detailed information on using the interface.

Procedure

Step 1 From the Cisco CRS Administration main window, choose **Applications > Configure Applications**. The Application Configuration window displays.

Step 2 Click the instance of Cisco CallManager AutoAttendant that you want to configure. The Cisco Script Application window displays

Step 3 You can change these settings:

- Description—The description of the application.
- ID—The application ID. The system reports the ID in Historical Reporting to identify this application.
- Maximum Number of Sessions—The maximum number of simultaneous callers that can use this automated attendant. This number should not exceed the number of CTI ports that were created for its use.
- Enabled—Indication that the automated attendant is running.
- Script—The script that will be running the application.
- welcomePrompt—The prompt that initially plays when the automated attendant answers the phone. See Configuring the Welcome Prompt, page 7-22, for information about how to upload prompts.
- MaxRetry—The number of times that a caller is returned to the Cisco CallManager AutoAttendant script main menu if caller encounters an error. The default specifies 3.
- operExtn—The extension of the phone that the operator will use.
- Default Script—The script that executes when an error occurs with the configured application script.

Step 4 Click **Update**.

Additional Information

See the "Related Topics" section on page 7-24

Configuring Prompts

Through Cisco CRS Administration Media Configuration, you can modify the prompts that Cisco CallManager AutoAttendant uses. You can also upload spoken names for each person in the organization, so callers receive spoken names rather than spelled-out names when the automated attendant is asking the caller to confirm which party they want.

These topics describe how to customize these features:

- Recording the Welcome Prompt, page 7-21
- Configuring the Welcome Prompt, page 7-22
- Uploading a Spoken Name, page 7-23

Recording the Welcome Prompt

Cisco CallManager AutoAttendant comes with a prerecorded, generic welcome prompt. You should record your own welcome prompt to customize your automated attendant for the specific role that it is to fulfill for your organization.

You can use any sound recording software to record the welcome prompt if the software can save the prompt in the required file format. You can record a different welcome prompt for each instance of Cisco CallManager AutoAttendant that you create.

This section describes how to record the welcome prompt by using Microsoft Sound Recorder. Save the prompt as a .wav file in CCITT (mu-law) 8-kHz, 8-bit, mono format. You must have a microphone and speakers on your system to use the software.

Procedure

Step 1 Start the Sound Recorder software; for example, by choosing **Start > Programs > Accessories > Entertainment > Sound Recorder**.

Step 2 Click the **Record** button and say your greeting into the microphone.

Step 3 When you finish the greeting, click the **Stop** button.

Step 4 To check your greeting

a. Click the **Rewind** button (also called “Seek to Start”) or drag the slider back to the beginning of the recording.

b. To play the recording, click the **Play** button. Rerecord your greeting until you are satisfied.

Step 5 When you are satisfied with your greeting, save the recording:

a. Choose **File>Save As**.

b. To set the recording options, click **Change**. (You can also do this by choosing **Properties** from the Sound Recorder File menu). Choose these options:

- Name—Choose **[untitled]**.
- Format—Choose **CCITT u-law**.
- Attributes—Choose **8.000 kHz, 8 Bit, Mono 7 kb/sec**.

You can save these settings to reuse later by clicking **Save As** and entering a name for the format.

c. To close the Sound Selection window, click **OK**.

d. Browse to the directory where you want to save the file, enter a file name, and click **Save**. Use the .wav file extension.

Additional Information

See the "Related Topics" section on page 7-24

Configuring the Welcome Prompt

Cisco CallManager AutoAttendant can only use welcome prompts that are stored on the Cisco CRS Engine. To configure your automated attendant to use a customized welcome prompt, you must upload it to the server and configure the appropriate Cisco CallManager AutoAttendant instance.

Tip To start Cisco CRS Administration, open http://*servername*/AppAdmin in your web browser, where *servername* specifies the DNS name or IP address of the application server. Click Help for detailed information on using the interface.

Procedure

Step 1 From the Cisco CRS Administration main menu, choose **Applications > Prompt Management**.

The Prompt Management window displays.

Step 2 From the Language Directory drop-down menu, choose the specific language and directory where the prompt should be uploaded.

Step 3 To add a new prompt

a. Click the **Add a new prompt** hyperlink.

The the Prompt File Name dialog box displays.

b. To open the Choose file dialog box, click **Browse**.

c. Navigate to the source .wav file folder and double-click the .wav file that you want to upload to the Cisco CRS Engine.

d. Confirm your choice in the **Destination File Name** field by clicking in the field.

e. To upload the .wav file, click **Upload**.

The system displays a message that the upload was successful.

f. Click the **Return to Prompt Management** hyperlink.

The window refreshes, and the file displays in the Prompt Management window.

Step 4 To replace an existing prompt with a new .wav file

a. Click the arrow in the Upload column for the prompt that you want to modify.

The Choose file dialog box opens.

b. Enter the name of the .wav file that you want to use to replace the existing prompt.

c. When you have provided the .wav file and prompt name information, click **Upload**.

Additional Information

See the "Related Topics" section on page 7-24

Uploading a Spoken Name

By default, Cisco CallManager AutoAttendant spells out the names of parties when it asks a caller to choose between more than one matching name or to confirm that the user wants to connect to the party. You can upload spoken names to the system, so your automated attendant plays spoken names rather than spelling them out.

To upload Cisco CallManager Spoken Names in your users voices, upload the corresponding .wav files into the directory by performing the following steps:

Procedure

Step 1 Ask users to record their names in the manner that is described in the "Recording the Welcome Prompt" section on page 7-21 and to save their files as *userId*.wav, where *userId* is their user name.

Step 2 Connect to Cisco CRS Administration. Choose **Tools > User Management**. The User Management window displays

Step 3 From the menu on the left, click the **Spoken Name Upload** link.

The Spoken Name Prompt Upload window displays. In the User ID field, enter a unique identifier of the user for which the spoken name is to be uploaded.

Step 4 In the Codec field, the codec that was chosen during installation for this CRS server automatically displays.

Step 5 In the Spoken Name (.wav) field, browse to the .wav file that you want to upload. Click it and then click **Open**

Step 6 From the Spoken Name Prompt Upload page, click **Upload**.

See the "Related Topics" section on page 7-24

Managing Cisco CallManager AutoAttendant

Use Cisco CRS Administration to manage Cisco CallManager AutoAttendant. Use the online help to learn how to use the interface and perform these tasks. Table 7-5 describes the management tasks.

Table 7-5 Managing Cisco CallManager AutoAttendant

Task	Purpose	Commands (from the Cisco CRS Administration main window)
Start and stop the Cisco CRS Engine	Make sure that the engine is running for your automated attendant to work. You can stop and restart the engine to help resolve or troubleshoot problems.	Choose **System > Control Center** and click the Cisco CRS Engine in the menu on the left. In the list that appears, find "CRS Engine". In the Status column, if a triangular button points to the right, you know that the engine is running. If a square shows in this column, you know that the engine is not running. To restart the engine, click the radio button next to "CRS Engine" and click **Restart**. If the engine is running and you want to stop it, click the radio button next to "CRS Engine" and click **Stop**.
Change the Cisco CRS Engine configuration	Modify the engine configuration to resolve problems.	Choose **System > System Parameters**.
Set up trace files	Set up trace files to collect troubleshooting information.	Choose **System > Tracing**; then, click **Trace File Configuration**. See the online help for detailed information.
View trace files	View trace files to see the results of your tracing.	Choose **System > Control Center**; then, click ***server name***. Click the **Server Traces** link. Choose the trace file that you created.
Monitor performance in real time	You can monitor the performance of the system while it is running if you install the real-time reporting monitor.	Choose **Tools > Real-Time Reporting**. See the online help for information on using Real Time Reporting.

Additional Information

See the "Related Topics" section on page 7-24

Related Topics

- Understanding Cisco CallManager AutoAttendant, page 7-1
- Cisco CallManager AutoAttendant Overview, page 7-2
- Installing and Upgrading the Customer Response Solutions (CRS) Engine, page 7-3
- Components of Cisco CallManager AutoAttendant, page 7-3
- Hardware and Software Requirements, page 7-3
- Installing or Upgrading Cisco CallManager AutoAttendant, page 7-4
- Installing Cisco CallManager AutoAttendant, page 7-4
- Configuring Cisco CallManager AutoAttendant and the CRS Engine, page 7-4

- Configuring a Cisco CallManager User for Cisco CallManager AutoAttendant, page 7-5
- Configuration Checklist for Cisco CallManager AutoAttendant, page 7-5
- Configuring Cisco CallManager, page 7-5
- Configuring the Cisco Customer Response Solutions Engine, page 7-9
- Cluster Setup, page 7-10
- Server Setup, page 7-11
- Adding a JTAPI Call Control Group, page 7-11
- Provisioning Cisco Media Termination Subsystem, page 7-15
- Adding a New Cisco CallManager AutoAttendant, page 7-16
- Configuring a JTAPI Trigger, page 7-17
- Customizing Cisco CallManager AutoAttendant, page 7-20
- Modifying an Instance of Cisco CallManager AutoAttendant, page 7-20
- Configuring Prompts, page 7-21
- Configuring the Welcome Prompt, page 7-22
- Recording the Welcome Prompt, page 7-21
- Uploading a Spoken Name, page 7-23
- Managing Cisco CallManager AutoAttendant, page 7-24

Barge and Privacy

The Barge and Privacy features work with each other. Both features work with only shared lines.

Barge adds a user to a call that is in progress. Pressing a softkey automatically adds the user (initiator) to the shared-line call (target), and the users currently on the call receive a tone (if configured). Barge supports built-in conference and shared conference bridges.

The administrator enables or disables Privacy setting. When Privacy is enabled, the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When Privacy is disabled, the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls. Administrators can configure Privacy for all devices or configure Privacy for each device. Users toggle the Privacy feature on or off.

This chapter provides the following information about Barge and Privacy:

- Introducing Barge and Privacy, page 8-1
- System Requirements for Barge and Privacy, page 8-5
- Interactions and Restrictions, page 8-6
- Installing and Activating Barge and Privacy, page 8-8
- Configuring Barge and Privacy, page 8-8
- Setting the Service Parameters for Barge and Privacy, page 8-10
- Related Topics, page 8-11

Introducing Barge and Privacy

The following sections describe Barge and Privacy.

- Barge, page 8-1
- Privacy, page 8-4

Barge

Barge allows a user to get added to a remotely active call that is on a shared line. Remotely active calls for a line comprise active (connected) calls that are made to or from another device that shares a directory number with the line. Barge supports this type of remote-in-use call.

Phones support Barge in two conference modes:

- Built-in conference bridge at the target device (the phone that is being barged). This mode uses the Barge softkey.
- Shared conference bridge. This mode uses the cBarge softkey.

By pressing the Barge or cBarge softkey in the remote in use call state, the user gets added to the call with all parties, and all parties receive a barge beep tone (if configured). If barge fails, the original call and status remain active.

If no conference bridge is available (built-in or shared), the barge request gets rejected, and a message displays at the barge initiator device.

Table 8-1 describes the differences between Barge with built-in conference bridge and shared conference.

Table 8-1 Built-In and Shared Conference Bridge Differences

Action	Using Barge Softkey (Built-In Conference Bridge at Target Device)	Using cBarge Softkey (Shared Conference Bridge)
The standard softkey template includes the softkey.	Yes	No
A media break occurs during barge setup.	No	Yes
User receives a barge setup tone, if configured.	Yes	Yes
To Conference displays as the name at the barge initiator phone.	To Barge	To Barge
To Conference displays as the name at the target phone.	To/From Other	To Barge
To Conference displays as the name at the other phones.	To/From Target	To Barge
A spinning circle displays on the right side of prompt status message at the target device.	Yes	No
Bridge supports a second barge setup to an already barged call.	No	Yes
Initiator releases the call.	No media interruption occurs for the two original parties.	Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.
Target releases the call.	Media break occurs to reconnect initiator with the other party as a point-to-point call.	Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.

Table 8-1 Built-In and Shared Conference Bridge Differences (continued)

Action	Using Barge Softkey (Built-In Conference Bridge at Target Device)	Using cBarge Softkey (Shared Conference Bridge)
Other party releases the call.	All three parties get released.	Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.
Target puts call on hold and performs direct transfer, Join, or Call Park.	Initiator gets released.	Initiator and the other party remain connected.

Barge Using Built-In Conference—Barge Softkey

You can use the Barge softkey only in the remote-in-use call state. A built-in conference bridge proves advantageous because neither a media interruption nor display changes to the original call occur when the barge is being set up. A spinning circle displays at the right side of the prompt status message window at the target device.

When the barge initiator releases the call, the barge call gets released between the barge initiator and target. The original call between the target device and the other party remains active. A barge disconnect tone (beep beep) plays to all remaining parties.

When the target device releases the call, the media between the barge initiator and the other party gets dropped briefly and then reconnects as a point-to-point call. The display changes at the barge initiator device to reflect the connected party.

When the other party releases the call, both the original call and the barge call get released.

When the barge initiator puts the call on hold, both the target device and the other party remain in the call.

When the target device puts the call on hold or in a conference or transfers it, the barge initiator gets released from the barge call while the original call also gets put on hold, in a conference, or transferred. The barge initiator can barge into a call again after the media gets reestablished at the target.

When the other party puts the call on hold or in a conference or transfers it, both the target device and the barge initiator remain in the call.

When network or Cisco CallManager failure occurs, the barge call gets preserved (like all active calls).

Some Cisco IP Phones (such as Model 7940 and 7960) have the built-in conference bridge capability, which barge uses.

Note Cisco IP Phone models 7940 and 7960 cannot support two media stream encryptions or SRTP streams simultaneously. To prevent instability due to this condition, the system automatically disables the built-in bridge for models 7940 and 7960 when the device security mode is set to encrypted. For more information, refer to the *Cisco CallManager Security Guide*.

The following settings activate or deactivate the built-in conference bridge:

- Enable or disable the built-in bridge by setting the Cisco CallManager clusterwide service parameter, Built-in Bridge Enable, to On or Off.

- Enable or disable the built-in bridge for each device by using the Built In Bridge drop-down list box in the Phone Configuration window (choose on, off, or default). On or off override the Built-in Bridge Enable service parameter. Choosing default uses the setting of the service parameter.

Note To use barge with a built-in bridge, ensure the preceding items are enabled, Privacy is disabled, and the Barge softkey is assigned to each device. Otherwise, to use shared conference bridge, assign the cBarge softkey to each device.

For more information, see the "Configuring Barge and Privacy" section on page 8-8.

Additional Information

See the "Related Topics" section on page 8-11.

Barge Using Shared Conference—cBarge Softkey

You can use the cBarge softkey only in the remote-in-use call state. No standard softkey template includes the cBarge softkey. To access the cBarge softkey, the administrator adds it to a softkey template and then assigns the softkey template to a device.

When cBarge gets pressed, a barge call gets set up by using the shared conference bridge, if available. The original call gets split and then joined at the conference bridge, which causes a brief media interruption. The call information for all parties gets changed to Barge.

The barged call becomes a conference call with the barge target device as the conference controller. It can add more parties to the conference or can drop any party.

When any party releases from the call, which leaves only two parties in the conference, the remaining two parties experience a brief interruption and then get reconnected as a point-to-point call, which releases the shared conference resource.

For more information, see the "Configuring Barge and Privacy" section on page 8-8.

Additional Information

See the "Related Topics" section on page 8-11.

Privacy

With Privacy, administrators can enable or disable the capability of users with phones that share the same line (DN) to view call status and to barge the call. Administrators enable or disable Privacy for each phone or for all phones in the cluster.

By default, the system enables Privacy for all phones in the cluster. To enable all phones with Privacy, leave the clusterwide service parameter to True and leave the phone privacy setting to default.

To configure certain phones with access to Privacy, administrators perform the following steps to enable or disable Privacy:

- Set a service parameter.
- Set the phone privacy setting to On.
- Add Privacy button to phone button template.
- Add the phone button template that has Privacy button to each device.

When the device that is configured for privacy registers with Cisco CallManager, the feature button on the phone that is configured with Privacy gets labeled, and the status shows through an icon. If the button has a lamp, it lights.

When the phone receives an incoming call, the user makes the call private (so the call information does not display on the shared line) by pressing the Privacy feature button. The Privacy feature button toggles between on and off.

Note When a Cisco CallManager database that contains the BargeEnabled parameter is upgraded from Cisco CallManager Release 3.3 to Release 4.0 or later, the system resets the privacy settings opposite the BargeEnabled setting.

Additional Information

See the "Related Topics" section on page 8-11.

System Requirements for Barge and Privacy

Barge and Privacy require the following software component to operate:

- Cisco CallManager 5.0

The following SIP and SCCP phones support Barge by using the Barge or cBarge softkey in any Cisco CallManager softkey template:

- Cisco IP Phones (Models 7905, 7912, 7920, 7940, 7941, 7960, 7961, 7970, 7971)

Note Cisco SCCP IP Phone (Models 7905 and 7912) support cBarge only. Cisco SIP IP Phone model 7940 and 7960 do not support cBarge or Barge.

The following SCCP phones support Privacy with the Privacy button on the phone button template:

- Cisco IP Phones (Models 7905, 7912, 7940, 7941, 7960, 7961, 7970, 7971)

The following SIP phones support Privacy with the Privacy button on the phone button template:

- Cisco IP Phones (Models 7940, 7941, 7960, 7961, 7970, 7971)

The following SCCP phones support the built-in conference bridge capability:

- Cisco IP Phones (Models 7940, 7960, 7970)

The following SIP phones support the built-in conference bridge capability:

- Cisco IP Phones (Models 7941, 7961, 7970, 7971)

Note If the phone does not support a Privacy button, by default, the privacy for that phone remains Off (all devices sharing a line with that phone will display the phone information).

Interactions and Restrictions

The following sections describe the interactions and restrictions for Barge and Privacy:

- Interactions, page 8-6
- Restrictions, page 8-6

Interactions

The following sections describe how Barge and Privacy interact with Cisco CallManager applications and call processing:

- Barge and cBarge, page 8-6
- Barge and Call Park, page 8-6
- Barge and Join, page 8-6

Barge and cBarge

Cisco recommends that you assign either the Barge or cBarge softkey to a softkey template. By having only one of these softkeys for each device, you can avoid confusion for users and potential performance issues.

Barge and Call Park

When the target parks the call, the barge initiator gets released (if using the built-in bridge), or the barge initiator and the other party remain connected (if using the shared conference).

Barge and Join

When the target joins the call with another call, the barge initiator gets released (if using the built-in bridge), or the barge initiator and the other party remain connected (if using the shared conference).

Restrictions

The following restrictions apply to Barge:

- To enhance performance, disable built-in bridge or turn on Privacy for those devices that do not have shared-line appearances or do not use barge.
- CTI does not support Barge through APIs that TAPI/JTAPI applications invoke. CTI generates events for Barge when it is invoked manually from an IP phone by using the Barge or cBarge softkey.
- Cisco recommends that you do not configure cBarge for a user who has Barge configured. Choose only one barge method for each user.
- The original call requires G.711 codec. If G.711 is not available, use cBarge instead.
- You can assign a softkey template, containing the barge softkey, to any IP Phone that uses softkeys; however, some IP Phone models do not support the Barge feature (Cisco IP Phone Model 7905 and Model 7912 support cBarge only).

- A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a busy tone plays on the phone where the user initiated the barge.
- Barge supports Cisco SIP IP Phones 7941, 7961, 7970, and 7971.

  If the initiator phone is configured for encryption, the barge initiator can barge into an authenticated or nonsecure call from the encrypted phone. After the barge occurs, Cisco CallManager classifies the call as nonsecure.

  If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call state equals encrypted.

  A user can barge into an authenticated call, even if the phone that is used to barge is nonsecure. The authentication icon continues to display on the authenticated devices in the call, even if the initiator phone does not support security.

Tip You can configure cbarge if you want barge functionality, but Cisco CallManager automatically classifies the call as nonsecure.

- If you configure encryption for Cisco IP Phone models 7960 and 7940, those encrypted devices cannot accept a barge request when they are participating in an encrypted call. When the call is encrypted, the barge attempt fails. A tone plays on the phone to indicate that the barge failed.

  A message displays in Cisco CallManager Administration when you attempt the following configuration:

  - In the Phone Configuration window, you choose **Encrypted** for the Device Security Mode (or System Default equals Encrypted), **On** for the Built In Bridge setting (or default setting equals On), and you click **Insert** or **Update** after you create this specific configuration.
  - In the Enterprise Parameter window, you update the Device Security Mode parameter.
  - In the Service Parameter window, you update the Built In Bridge Enable parameter.

The following restrictions apply to Privacy:

- To enhance performance, disable built-in bridge or turn on Privacy for those devices that do not have shared-line appearances or do not use barge.
- CTI does not support Privacy through APIs that TAPI/JTAPI applications invoke. CTI generates events when Privacy gets enabled or disabled from an IP phone by using the Privacy feature button.
- Privacy supports Cisco SIP IP Phones 7941, 7961, 7970, and 7971.

The following restriction applies to built-in conference bridge:

- To enhance performance, disable built-in bridge or turn on Privacy for those devices that do not have shared-line appearances or do not use barge.
- The initiator cannot park a call, redirect a call, or use any feature that is using the CTI/JTAPI/TSP interface. The system supports only hold and unhold.
- Built-in conference bridge supports Cisco SIP IP Phones 7941, 7961, 7970, and 7971.

Installing and Activating Barge and Privacy

Barge and Privacy system features come standard with Cisco CallManager software. The administrator activates the features after installation to make them available for system use. The following sections provide information about activating the features:

- Activating Barge with Built-In Conference Bridge, page 8-8
- Activating cBarge with Shared Conference Bridge, page 8-8
- Activating Privacy, page 8-8

Activating Barge with Built-In Conference Bridge

To activate Barge with built-in conference bridge, add the Barge softkey to a softkey template, assign the softkey template to a device, set the Built-in Bridge Enable service parameter to On, and set the party entrance tone to True. See the "Barge Configuration Checklist" section on page 8-9 for details.

Note To set Barge with built-in conference bridge for all users, set the Built-in Bridge Enable service parameter to On. To set Barge with built-in conference bridge for individual users, set the Built in Bridge field to On in the Phone Configuration window.

Activating cBarge with Shared Conference Bridge

To activate Barge with shared conference bridge, add the cBarge softkey to a softkey template, assign the softkey template to a device, and set the party entrance tone to True. See the "Barge Configuration Checklist" section on page 8-9 for details.

Activating Privacy

The system automatically activates Privacy in the Cisco CallManager cluster because the Privacy Setting service parameter is set to True and the phone has the Privacy setting at Default. The administrator must also add Privacy to a phone button template and assign the phone button template to a device. See the "Privacy Configuration Checklist" section on page 8-10 for details.

Configuring Barge and Privacy

This section contains the following information:

- Barge Configuration Checklist, page 8-9
- Privacy Configuration Checklist, page 8-10
- Setting the Service Parameters for Barge and Privacy, page 8-10

Barge Configuration Checklist

Table 8-2 provides a checklist to configure Barge with built-in conference bridge.

Table 8-2 Barge with Built-In Conference Bridge Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	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.	Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*
Step 2	Set the following optional Cisco CallManager service parameters: • To enable Barge for all users, set the Built-In Bridge Enable clusterwide service parameter to On **Note** If this parameter is set to Off, configure Barge for each phone by setting the Built in Bridge field in Phone Configuration • Set the Party Entrance Tone clusterwide service parameter to True (required for tones)	Configuring Service Parameters for a Service on a Server, *Cisco CallManager Administration Guide* Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*
Step 3	In the End User Configuration window for each user that is allowed to access the Barge with built-in conference bridge feature, associate the device that has the Barge softkey template that is assigned to it.	End User Configuration, *Cisco CallManager Administration Guide*
Step 4	Notify users that the Barge feature is available.	Refer to the phone documentation for instructions on how users access Barge on their Cisco IP Phone.

Table 8-3 provides a checklist to configure Barge with shared conference bridge.

Table 8-3 Barge with Shared Conference Bridge (cBarge) Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	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.	Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*
Step 2	Set the optional clusterwide service parameter Party Entrance Tone to True (required for tones).	Configuring Service Parameters for a Service on a Server, *Cisco CallManager Administration Guide*
Step 3	In the End User Configuration window for each user that is allowed to access the cBarge with shared conference bridge feature, associate the device that has the cBarge softkey template that is assigned to it.	End User Configuration, *Cisco CallManager Administration Guide*
Step 4	Notify users that the cBarge feature is available.	Refer to the phone documentation for instructions on how users access cBarge on their Cisco IP Phone.

Privacy Configuration Checklist

Table 8-4 provides a checklist to configure Privacy.

Table 8-4 Privacy Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	If all phones in the cluster need access to Privacy, keep the setting of the Privacy Setting clusterwide service parameter to True (default) and keep the Privacy field in the Phone Configuration window to Default. Continue with the following steps. If only certain phones in the cluster need access to Privacy, set the Privacy Setting service parameter to False and set the Privacy field in the Phone Configuration window to On. Continue with the following steps.	Configuring Service Parameters for a Service on a Server, *Cisco CallManager Administration Guide* Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*
Step 2	For each phone button template that has Privacy, add Privacy to one of the feature buttons (some phone models use the Private button).	Phone Button Template Configuration, *Cisco CallManager Administration Guide*
Step 3	For each phone user that wants Privacy, choose the phone button template that contains the Privacy feature button.	Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*
Step 4	In the End User Configuration window, for each user that does not want information about the shared-line appearances to display, associate the device that has the Privacy feature button that is assigned to it.	End User Configuration, *Cisco CallManager Administration Guide*
Step 5	Notify users that the Privacy feature is available.	Refer to the phone documentation for instructions on how users access Privacy on their Cisco IP Phone.

Setting the Service Parameters for Barge and Privacy

Cisco CallManager provides three clusterwide service parameters: Built In Bridge Enable for the built-in conference bridge capability, Privacy Setting for the Privacy feature, and Party Entrance Tone for the tones that are played during barge.

- Built In Bridge Enable—Default specifies Off. This parameter enables or disables the built-in conference bridge capability for phones that use the Barge softkey. Set this parameter for each server in a cluster that has the Cisco CallManager service and Barge configured. If Built in Bridge is set to On in Phone Configuration, the service parameter setting gets overridden.
- Privacy Setting—Default specifies True. This parameter enables or disables the Privacy feature for phone users who do not want to display information on shared-line appearances. Set this parameter for each server in a cluster that has the Cisco CallManager service and Privacy configured. If only certain phones need the Privacy feature, set the service parameter to False and set the Privacy field to On in Phone Configuration.

  If the Privacy field in the Phone Configuration window is set to default, the phone uses the setting that is configured in the Privacy Setting service parameter.
- Party Entrance Tone—Default specifies False. This parameter enables or disables the tones that play during barge. Set this parameter for each server in a cluster that has the Cisco CallManager service and Barge (with tones) configured.

Related Topics

- Cisco IP Phone administration documentation for Cisco CallManager
- Cisco IP Phone user documentation and release notes
- *Cisco CallManager Security Guide*
- Phone Button Template Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Softkey Template Configuration, *Cisco CallManager Administration Guide*
- End User Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phones, *Cisco CallManager System Guide*
- Configuring Service Parameters for a Service on a Server, *Cisco CallManager Administration Guide*
- Configuring Phone Button Templates, *Cisco CallManager Administration Guide*
- Privacy Configuration Checklist, page 8-10

CHAPTER 9

Call Park

The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the Cisco CallManager system (for example, a phone in another office or in a conference room). If you are on an active call at your phone, you can park the call to a call park extension by pressing the Park softkey or the Call Park button. Someone on another phone in your system can then dial the call park extension to retrieve the call.

You can define either a single directory number or a range of directory numbers for use as call park extension numbers. You can park only one call at each call park extension number.

This chapter provides the following information about call park:

- Introducing Call Park, page 9-1
- System Requirements for Call Park, page 9-4
- Interactions and Restrictions, page 9-4
- Installing and Activating Call Park, page 9-6
- Configuring Call Park, page 9-6
- Setting the Service Parameters for Call Park, page 9-7
- Finding a Call Park Number, page 9-7
- Configuring a Call Park Number, page 9-9
- Deleting a Call Park Number, page 9-11
- Related Topics, page 9-12

Introducing Call Park

The Call Park feature works within a Cisco CallManager cluster, and each Cisco CallManager in a cluster must have call park extension numbers defined. (For information about using call park across clusters, see the "Using Call Park Across Clusters" section on page 9-2.) You can define either a single directory number or a range of directory numbers for use as call park extension numbers. Ensure that the directory number or range of numbers is unique.

Valid call park extension numbers comprise integers and the wildcard character, X. You can configure a maximum of XX in a call park extension number (for example, 80XX), which provides up to 100 call park extension numbers. When a call gets parked, Cisco CallManager chooses the next call park extension number that is available and displays that number on the phone.

Cisco CallManager can park only one call at each call park extension number.

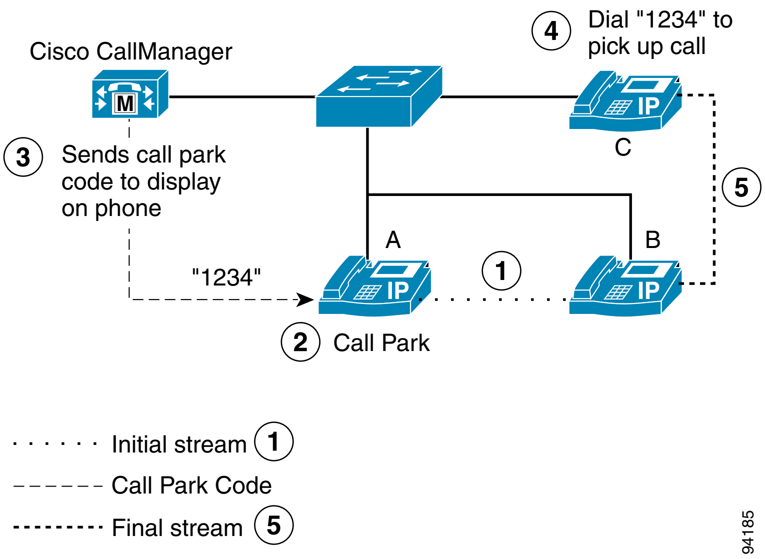
Note If users will use call park across servers in a cluster, ensure each Cisco CallManager server in a cluster has call park extension numbers that are configured. See the "Configuring a Call Park Number" section on page 9-9 for configuration details.

Using the Call Park Feature

Figure 9-1 illustrates the call park process.

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 CallManager 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 (so he can 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 call between phones C and B.

Figure 9-1 Call Park Process



Using Call Park Across 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 CallManager cluster. Additionally, you must ensure that calling search spaces and partitions are properly configured. See the following example.

Example of Retrieving Parked Calls from Another Cluster

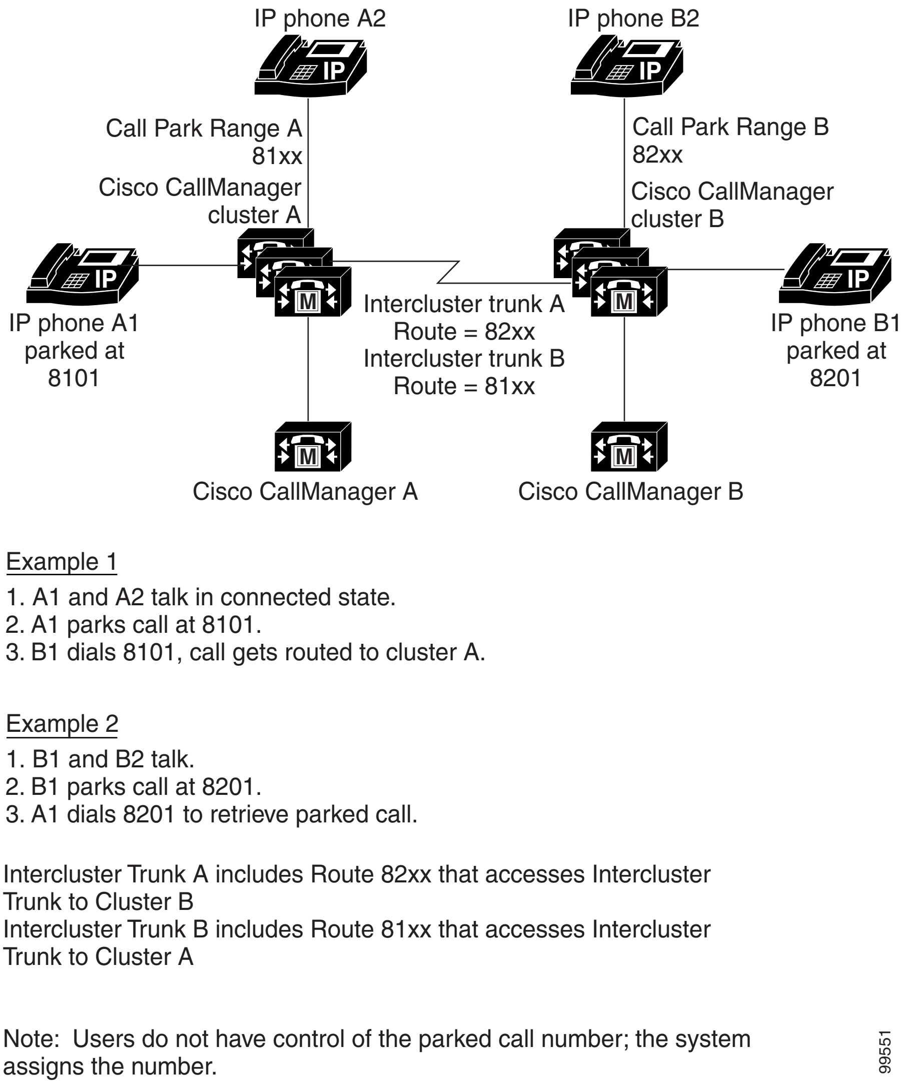
Two clusters exist in the network (cluster A and cluster B). Cluster A includes user A1 and user A2. Cluster B includes user B1 and user B2.

Cluster A includes call park numbers in the range of 81xx. Cluster B includes call park numbers in the range of 82xx, which the administrator configured.

Cluster A includes route patterns that are configured to other cluster park ranges as 82xx (routes to Cluster B). Cluster B includes route patterns that are configured to other cluster park ranges as 81xx (routes to Cluster A).

When user A1 parks a call at 8101, all users (which have correct partitions configured) in Cluster A and Cluster B can retrieve the parked call because of the route pattern configuration. When user B1 parks a call at 8202, all users (which have correct partitions configured) in Cluster A and Cluster B can retrieve the parked call because of the route pattern configuration. See Figure 9-2.

Figure 9-2 Retrieving Parked Calls by Using Intercluster Trunks



Example 1

1. A1 and A2 talk in connected state.
2. A1 parks call at 8101.
3. B1 dials 8101, call gets routed to cluster A.

Example 2

1. B1 and B2 talk.
2. B1 parks call at 8201.
3. A1 dials 8201 to retrieve parked call.

Intercluster Trunk A includes Route 82xx that accesses Intercluster Trunk to Cluster B
Intercluster Trunk B includes Route 81xx that accesses Intercluster Trunk to Cluster A

Note: Users do not have control of the parked call number; the system assigns the number.

System Requirements for Call Park

To operate, call park requires the following software component:

- Cisco CallManager 5.0

The following SCCP and SIP phones support call park with the Park softkey in the Standard User and Standard Feature softkey templates:

- Cisco IP Phones (models 7941, 7961, 7970, 7971)

The following SCCP phones support call park with the Park softkey in the Standard User and Standard Feature softkey templates:

- Cisco IP Phones (models 7905, 7912, 7920, 7940, 7960)

The following SCCP phones support call park with the Call Park button on the phone button template:

- Cisco IP Phone model 30 (30 SP+ and 30 VIP)
- Cisco IP Phone model 12 (12 S, 12 SP, 12 SP+)
- Cisco IP Phone model 7910

Interactions and Restrictions

The following sections describe the interactions and restrictions for call park:

- Interactions, page 9-4
- Restrictions, page 9-6

Interactions

The following sections describe how call park interacts with Cisco CallManager applications and call processing:

- CTI Applications, page 9-4
- Music On Hold, page 9-5
- Route Plan Report, page 9-5
- Calling Search Space and Partitions, page 9-5
- Immediate Divert, page 9-5
- Barge, page 9-5

CTI Applications

CTI applications (for example, Attendant Console) access call park functionality, including monitoring activity on call park DNs. To monitor a call park DN, an application or end user that is associated with the CTI application must be added to the Standard CTI Allow Call Park Monitoring user group.

Refer to the "Configuration Checklist for Cisco CallManager Attendant Console" section on page 16-16 for details.

Music On Hold

Music on hold allows users to place calls on hold with music that a streaming source provides. Music on hold allows two types of hold:

- User hold—The system invokes this type of hold when a user presses the Hold button or Hold softkey.
- Network hold—This type of hold takes place when a user activates the transfer, conference, or call park feature, and the hold automatically gets invoked.

Route Plan Report

The route plan report displays the patterns and directory numbers that are configured in Cisco CallManager. Use the route plan report to look for overlapping patterns and directory numbers before assigning a directory number to call park. Refer to the Route Plan Report chapter in the *Cisco CallManager Administration Guide*.

Calling Search Space and Partitions

Assign the Call Park directory number or range to a partition to limit call park access to users on the basis of the device calling search space. See Calling Search Space Configuration and Partition Configuration in the *Cisco CallManager Administration Guide*.

Immediate Divert

Call park supports Immediate Divert (iDivert softkey). For example, user A calls user B, and user B parks the call. User B retrieves the call and then decides to send the call to voice-messaging mailbox by pressing the iDivert softkey. User A receives the voice-messaging mailbox greeting of user B.

Barge

The following paragraphs describe the differences between Barge and cBarge with call park.

Barge with Call Park

The target phone (the phone that is being barged upon) controls the call. The barge initiator “piggy backs” on the target phone. The target phone includes most of the common features, even when the target is being barged; therefore, the barge initiator has no feature access. When the target parks a call, the barge initiator then must release its call (the barge).

cBarge with Call Park

The target and barge initiator act as peers. The cBarge feature uses a conference bridge, which makes it behave similar to a MeetMe conference. Both phones (target and barge initiator) have full access to their features.

Restrictions

The following restrictions apply to call park:

- Cisco CallManager can park only one call at each call park extension number.
- Ensure each call park directory number, partition, and range is unique within the Cisco CallManager cluster.
- Each Cisco CallManager to which devices are registered needs its own unique call park directory number and range.
- Cisco IP Phone 7902 cannot park a call (retrieval of parked calls only).

See the "Configuring a Call Park Number" section on page 9-9 for configuration details.

Installing and Activating Call Park

Call park, a system feature, comes standard with Cisco CallManager software. It does not require special installation.

Configuring Call Park

This section contains the following information:

- Call Park Configuration Checklist, page 9-6
- Setting the Service Parameters for Call Park, page 9-7
- Finding a Call Park Number, page 9-7
- Configuring a Call Park Number, page 9-9
- Deleting a Call Park Number, page 9-11
- Troubleshooting Call Park, page 9-11

Call Park Configuration Checklist

Table 9-1 provides a checklist to configure Call Park.

Table 9-1 Call Park Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure a partition for call park extension numbers to make partition available only to users who have the partition in their calling search space.	Configuring a Partition, *Cisco CallManager Administration Guide* Media Termination Point Configuration, *Cisco CallManager Administration Guide*
Step 2	Configure a unique call park number or define a range of call park extension numbers for each Cisco CallManager in the cluster.	Configuring a Call Park Number, page 9-9

Table 9-1 Call Park Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 3	Add all servers that call park uses to the appropriate Cisco CallManager group. **Note** Servers and Cisco CallManagers get configured during installation.	Cisco CallManager Group Configuration, *Cisco CallManager Administration Guide*
Step 4	Assign the Standard User softkey template to each device that has call park access. For phones that do not use softkeys, the phone button template with the Call Park button automatically gets configured.	Softkey Template Configuration, *Cisco CallManager Administration Guide*
Step 5	In the User Group Configuration window, assign application and end users to the Standard CTI Allow Call Park Monitoring user group. This applies only to users associated with CTI applications requiring Call Park monitoring capability (for example, Attendant Console).	Adding Users to a User Group, *Cisco CallManager Administration Guide*
Step 6	Notify users that the call park feature is available.	Refer to the phone documentation for instructions on how users access call park features on their Cisco IP Phone.

Setting the Service Parameters for Call Park

Cisco CallManager provides two clusterwide service parameters for call park: Call Park Display Timer and Call Park Reversion Timer. Each service parameter includes a default and requires no special configuration.

- Call Park Display Timer—Default specifies 10 seconds. This parameter determines how long a call park number displays on the phone that parked the call. Set this timer for each server in a cluster that has the Cisco CallManager service and call park configured.
- Call Park Reversion Timer—Default specifies 60 seconds. This parameter determines the time that a call remains parked. Set this timer for each server in a cluster that has the Cisco CallManager service and call park configured. When this timer expires, the parked call returns to the device that parked the call.

Note To set the timers, choose **System > Service Parameters** and update the Call Park Display Timer and the Call Park Reversion Timer fields in the **Clusterwide Parameters (Feature-General)** pane.

Finding a Call Park Number

Because you may have several call park numbers in your network, Cisco CallManager lets you locate specific call park numbers on the basis of specific criteria. Use the following procedure to locate call park numbers.

Note During your work in a browser session, Cisco CallManager Administration retains your call park number search preferences. If you navigate to other menu items and return to this menu item, Cisco CallManager Administration retains your call park number search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Call Park**.

The Find and List Call Park Numbers window displays. Use the two drop-down list boxes to search for a call park number.

Step 2 From the first Find Call Park Numbers where drop-down list box, choose one of the following criteria:

- Number
- Partition
- Description
- CallManager

Note The criterion that you choose in this drop-down list box specifies how the list of call park numbers that your search generates will be sorted.

From the second Find Call Park Numbers where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

Tip To find all call park numbers that are registered in the database, click **Find** without entering any search text.

A list of discovered call park numbers displays by

- Call Park Number icon
- Call Park Number
- Partition
- Description
- CallManager

Step 4 From the list of records, click the Call Park Number that matches your search criteria.

The window displays the call park number that you choose.

Additional Information

See the "Related Topics" section on page 9-12.

Configuring a Call Park Number

This section describes how to add, copy, and update a single call park extension number or range of extension numbers.

Procedure

Step 1 Choose **Call Routing** > **Call Park**.

Step 2 Perform one of the following tasks:

- To add a new Call Park Number, click **Add New**.
- To copy a Call Park Number, use the procedure in the "Finding a Call Park Number" section on page 9-7 to locate the call park number or range of numbers. Click the Copy icon.
- To update a Call Park Number, use the procedure in the "Finding a Call Park Number" section on page 9-7 to locate the call park number or range of numbers.

The Call Park Number Configuration window displays.

Step 3 Enter or update the appropriate settings as described in Table 9-2.

Step 4 To save the new or changed call park numbers in the database, click **Save**.

Additional Information

See the "Related Topics" section on page 9-12.

Call Park Configuration Settings

Table 9-2 describes the call park configuration settings. For related procedures, see the "Related Topics" section on page 9-12.

Table 9-2 Call Park Configuration Settings

Field	Description
Call Park Number/Range	Enter the call park extension number. You can enter literal digits or the wildcard character X (the system allows one or two Xs). For example, enter 5555 to define a single call park extension number of 5555 or enter 55XX to define a range of call park extension numbers from 5500 to 5599. **Note** You can create a maximum of 100 call park numbers with one call park range definition. Make sure that the call park numbers are unique. **Note** You cannot overlap call park numbers between Cisco CallManager servers. Ensure that each Cisco CallManager server has its own number range.
Description	Provide a brief description of this call park number.
Partition	If you want to use a partition to restrict access to the call park numbers, choose the desired partition from the drop-down list box. If you do not want to restrict access to the call park numbers, choose <None> for the partition. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (**...**) displays next to the drop-down list box. Click the **...** button to display the Select Partition window. Enter a partial partition name in the **List items where Name contains** field. Click the desired partition name in the list of partitions that displays in the **Select item to use** box and click **OK**. **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and update the Max List Box Items field under **CCMAdmin Parameters**. **Note** Make sure that the combination of call park extension number and partition is unique within the Cisco CallManager cluster.
Cisco CallManager	Using the drop-down list box, choose the Cisco CallManager to which these call park numbers apply. **Note** You can create a maximum of 100 call park numbers with one call park range definition. Make sure that the call park numbers are unique. **Note** You cannot overlap call park numbers between Cisco CallManager servers. Ensure that each Cisco CallManager server has its own number range.

Deleting a Call Park Number

This section describes how to delete call park numbers from the Cisco CallManager database.

Procedure

Step 1 Using the procedure in the "Finding a Call Park Number" section on page 9-7, locate the call park number or range of numbers.

Step 2 Click the call park number or range of numbers that you want to delete.

Step 3 Click **Delete**.

Note You can delete multiple call park numbers from the Find and List Call Park Numbers window by checking the check boxes next to the appropriate call park numbers and clicking **Delete Selected**. You can delete all call park numbers in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the "Related Topics" section on page 9-12.

Troubleshooting Call Park

Table 9-3 provides troubleshooting recovery tips for common call park problems.

Table 9-3 Troubleshooting Tips for Call Park

Problem Description	Recommended Action
User cannot park calls. When the user presses the Park softkey or feature button, the call does not get parked.	Ensure that a unique call park number is assigned to each Cisco CallManager in the cluster. See the "Configuring a Call Park Number" section on page 9-9. The partition that is assigned to the call park number does not match the partition that is assigned to the phone directory number. See the "Configuring a Call Park Number" section on page 9-9 and the "Configuring a Directory Number" section in the *Cisco CallManager Administration Guide*.
The call park number does not display long enough for the user.	Set the Call Park Display Timer to a longer duration. See the "Setting the Service Parameters for Call Park" section on page 9-7.

Additional Information

See the "Related Topics" section on page 9-12.

Related Topics

- Call Park, page 9-1
- Configuring a Call Park Number, page 9-9
- Finding a Call Park Number, page 9-7
- Deleting a Call Park Number, page 9-11
- Troubleshooting Call Park, page 9-11
- Phone Button Template Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Partition Configuration, *Cisco CallManager Administration Guide*
- Media Termination Point Configuration, *Cisco CallManager Administration Guide*
- Route Plan Report, *Cisco CallManager Administration Guide*
- Softkey Template Configuration, *Cisco CallManager Administration Guide*
- End User Configuration, *Cisco CallManager Administration Guide*
- User Group Configuration, *Cisco CallManager Administration Guide*
- Clustering, *Cisco CallManager System Guide*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- Cisco IP Phone user documentation and release notes (all models)

Call Pickup Group

The Call Pickup feature allows users to answer calls that come in on a directory number other than their own. The "Introducing Call Pickup Group" section on page 10-1 describes this feature.

This section covers the following topics:

- Introducing Call Pickup Group, page 10-1
- System Requirements for Call Pickup Group, page 10-3
- Interactions and Restrictions, page 10-4
- Installing and Activating Call Pickup Group, page 10-6
- Configuring Call Pickup Group, page 10-6
- Related Topics, page 10-15

Introducing Call Pickup Group

Cisco IP Phones provide three types of call pickup: call pickup, group call pickup, and other group call pickup.

- Call pickup—Allows users to pick up incoming calls within their own group. Cisco CallManager automatically dials the appropriate call pickup group number when the user activates this feature from a Cisco IP Phone. Use the softkey, PickUp, for this type of call pickup.
- Group call pickup—Allows users to pick up incoming calls in another group. User must dial the appropriate call pickup group number when activating this feature from a Cisco IP Phone. Use the softkey, GPickUp, for this type of call pickup.

Note The same procedures apply for configuring call pickup and group call pickup features. Group call pickup numbers apply to lines or directory numbers.

- Other group call pickup—Allows users to pick up incoming calls in a group that is associated with their own group. The Cisco CallManager automatically searches for the incoming call 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, B, and then C. First, group X picks up incoming call in group A, though a call may have come in earlier in group C than the incoming call in group A.

Note Usually, within the same group, the longest alerting call (longest ringing time) gets 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 idle and offhook call states make the three softkeys, PickUp, GPickUp, and oPickup, available. The administrator must modify the standard softkey template to include these softkeys for the users to invoke the Call Pickup feature. See the "Call Pickup Group Configuration Checklist" section on page 10-6 and the "Other Group Call Pickup Configuration Checklist" section on page 10-8.

Auto Call Pickup

You can automate call pickup, group pickup, and other group pickup by enabling the service parameter Auto Call Pickup Enabled.

When this parameter is enabled, Cisco CallManager 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 in the user's own group. When the user presses the Pickup softkey on the phone, Cisco CallManager locates the incoming call in the group and completes the call connection. If automation is not enabled, the user must press the softkeys, Pickup and Answer, to make the call connection.

Auto group call pickup connects users to an incoming call in another pickup group. The user presses the GPickUp softkey on the phone, then dials the DN of that other pickup group. Upon receiving the DN, Cisco CallManager completes the call connection. If auto group call pickup is not enabled, the user must press the GPickUp softkey, dial the DN of another pickup group, and answer the call to make the connection.

Auto other group call pickup connects user to an incoming call in a group that is associated with the user's own group. The user presses the oPickup softkey on the phone. Cisco CallManager automatically searches for the incoming call in the associated groups in the sequence that the administrator enters in the Pickup Group Configuration window and completes the call connection after the call is found. If automation is not enabled, the user must press the softkeys, oPickup and Answer, to make the call connection.

Note CTI applications supports monitoring the party whose call is picked up. CTI applications do not support monitoring the pickup requester or the destination of the call that is picked up. Hence, Cisco IPMA does not support auto call pickup (one-touch call pickup).

Call Pickup No Answer

When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the call forward configured on the phone, when one of the pickup softkeys is pressed, gets ignored. If the call pickup requestor does not answer the call, the original call is restored after the pickup no answer timer expires.

Call Pickup Busy

When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the original call is restored while the call pickup requestor phone is busy.

Call Pickup No Bandwidth

When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the original call is restored when there is no bandwidth between the call originator and requestor phones.

Additional Information

See the "Related Topics" section on page 10-15.

Using Call Pickup Features with Partitions to Restrict Access

You can restrict access to call pickup groups by assigning a partition to the call pickup group number. When this configuration is used, only the phones that have a calling search space 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.

- If call pickup group numbers are assigned to a partition, only those phones that can dial numbers in that partition can use the call pickup group.
- If partitions represent tenants in a multitenant configuration, make sure that the pickup groups are assigned to the appropriate partition for each tenant.

A multitenant configuration provides an example of using partitions with call pickup groups. Assign the pickup groups to the appropriate partition for each tenant, and the group number will not be visible to other tenants.

System Requirements for Call Pickup Group

To operate, call pickup group requires the following software component:

- Cisco CallManager 5.0

The following SCCP and SIP phones support call pickup group with Pick Up (PickUp) and Group Pickup (GPickUp) softkeys in the Standard User and Standard Feature softkey templates:

- Cisco IP Phones (models 7941, 7961, 7970, 7971)

The following SCCP phones support call pickup group with the Pick Up (PickUp) and Group Pickup (GPickUp) softkeys in the Standard User and Standard Feature softkey templates:

- Cisco IP Phones (models 7905, 7912, 7920, 7940, 7960)

Note The administrator must add the Other Pickup (oPickup) softkey to the softkey templates.

Interactions and Restrictions

The following sections describe the interactions and restrictions for call pickup:

- Interactions, page 10-4
- Restrictions, page 10-5

Interactions

The following sections describe how call pickup group interacts with Cisco CallManager applications and call processing:

- Route Plan Report, page 10-4
- Calling Search Space and Partitions, page 10-4
- Time of Day, page 10-4
- Call Accounting, page 10-5
- Dependency Records, page 10-5

Route Plan Report

The route plan report displays the patterns and directory numbers that are configured in Cisco CallManager. Use the route plan report to look for overlapping patterns and directory numbers before assigning a directory number to call pickup group. Refer to the Route Plan Report chapter in the *Cisco CallManager Administration Guide*.

Calling Search Space and Partitions

Assign a partition to the Call Pickup Group number to limit call pickup access to users on the basis of the device calling search space. Refer to Calling Search Space Configuration and Partition Configuration in the *Cisco CallManager Administration Guide*.

Time of Day

To pick up calls from a group that is associated with your own group, you must configure the calling search space, partition, and the Time of Day (TOD) parameter for members in the associated group to be active and able to accept calls within the same time period as your own group. TOD associates a time stamp to the calling search space and partition.

For example, a partition, ABC, remains active between 9 am to 5 pm. A calling search space, cssABC, contains partition ABC. A pickup group, pickABC contains phone 1 and phone 2. Phone 1 and phone 2 reside in the same calling search space, cssABC. If phone 1 rings at 5:30 pm and phone 2 tries to pick up the call, this attempt fails because the partition is not active after 5 pm. If phone 1 rings at 9:30 am, phone 2 can pick up the call.

Call Accounting

Call Pickup Groups interact with call accounting.

- When a call pickup occurs via auto call pickup, the system generates two call detail records (CDRs). One CDR applies to the original call that is cleared, and another CDR applies to the requesting call that is connected.
- When a call pickup occurs via non-auto call pickup, the system generates one call detail record, which applies to the requesting call that is connected.
- A CDR search returns all CDRs that match a specific time range and other search criteria as specified. If users are interested in the type of call that is associated with a particular CDR, the search result displays a call type field that indicates whether the call is a pickup call.

Dependency Records

If you need to find devices to which a specific call pickup number is assigned, click the Dependency Records link that the Cisco CallManager Administration Pickup Group Configuration window provides. The Dependency Records Summary window displays information about devices that are using the call pickup number.

If a pickup group is associated with other pickup groups, the dependency record of the pickup group shows the association information. For example, if pickup group A is associated with pickup group B and pickup group C, the dependency record of pickup group A shows the information on the association of pickup group A to pickup group B and C.

To find out more information about the devices, click the device, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

For more information about Dependency Records, refer to "Accessing Dependency Records" in the *Cisco CallManager Administration Guide*.

Restrictions

The following restrictions apply to call pickup group:

- Although different lines on a phone can be assigned to different call pickup groups, Cisco does not recommend this setup because it can be confusing to users.
- You cannot delete a call pickup group number when it is assigned to a line or directory number. To determine which lines are using the call pickup number, use Dependency Records. To delete a call pickup group number, reassign a new call pickup group number to each line or directory number.
- When you update a call pickup group number, Cisco CallManager automatically updates all directory numbers that are assigned to that call pickup group.

- Cisco CallManager Attendant Console does not work with the call pickup group feature. The attendant console user interface cannot appropriately handle calls coming from or made to phones belonging to a call pickup group due to JTAPI and CTI limitations.

Installing and Activating Call Pickup Group

Call pickup group, a system feature, comes standard with Cisco CallManager software. It does not require special installation.

Configuring Call Pickup Group

This section contains the following information:

- Call Pickup Group Configuration Checklist, page 10-6
- Other Group Call Pickup Configuration Checklist, page 10-8
- Setting the Service Parameters for Call Pickup Group, page 10-9
- Finding a Call Pickup Group, page 10-10
- Configuring a Call Pickup Group, page 10-11
- Call Pickup Group Configuration Settings, page 10-12
- Deleting a Call Pickup Group, page 10-13
- Defining a Pickup Group for Other Group Call Pickup, page 10-13
- Assigning A Call Pickup Group to Directory Numbers, page 10-14

Call Pickup Group Configuration Checklist

Table 10-1 provides a checklist to configure Call Pickup Group.

Table 10-1 Call Pickup Group Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure partitions if you will be using them with call pickup groups.	Configuring a Partition, *Cisco CallManager Administration Guide* Using Call Pickup Features with Partitions to Restrict Access, page 10-3
Step 2	Configure a call pickup group. Make sure that the name and number are unique.	Configuring a Call Pickup Group, page 10-11

Table 10-1 Call Pickup Group Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 3	Assign the call pickup group that you created in Step 2 to the directory numbers that are associated with phones on which you want to enable call pickup: • Only directory numbers that are assigned to a call pickup group can use the Call Pickup feature. • If partitions are used with call pickup numbers, make sure that the directory numbers that are assigned to the call pickup group have a calling search space that includes the appropriate partitions.	Assigning A Call Pickup Group to Directory Numbers, page 10-14
Step 4	Add a call pickup or group call pickup button to the phone button templates, if needed. You only need to do this for Cisco IP Phone model 12 SP, 12 SP+, and 30 VIP.	Configuring Phone Button Templates, *Cisco CallManager Administration Guide*
Step 5	Assign the Standard User or Standard Feature softkey template to the phone that will be using the Pickup (PickUp) and Group Call Pickup (GPickUp) softkeys. **Note** To restrict calls to be picked up by phones within its own group only, deny the GPickUp or oPickup softkeys in the softkey template by moving them to the Unselected box that is in the Softkey Configuration window.	Assigning Softkey Templates to IP Phones, *Cisco CallManager Administration Guide*
Step 6	If you want automatic call answering for call pickup groups, enable the Auto Call Pickup Enabled service parameter by choosing the value True. The default specifies False.	Auto Call Pickup, page 10-2. Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 7	If the Auto Call Pickup Enabled service parameter is false, enter a value for the Call Pickup No Answer Timer service parameter. This parameter controls the amount of time that a call takes to get restored if a call is picked up by using call pickup, group call pickup, or other group call pickup.	Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 8	Enter a value for the Pickup Locating Timer service parameter. This parameter controls the time for call selection for call pickup, group call pickup, and other group call pickup.	Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 9	Notify users that the Call Pickup feature is available.	Refer to the phone documentation for instructions on how users access the Call Pickup feature on their Cisco IP Phone.

Additional Information

See the "Related Topics" section on page 10-15.

Other Group Call Pickup Configuration Checklist

Table 10-2 provides a checklist to configure other group call pickup.

Table 10-2 Other Group Call Pickup Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure a list of associated groups that can be chosen from all pickup groups. The list can include up to ten groups.	Defining a Pickup Group for Other Group Call Pickup, page 10-13
Step 2	Configure Calling Search Space and TOD parameters for members of the associated groups to your group.	Calling Search Space Configuration, *Cisco CallManager Administration Guide* Time-of-Day Routing, *Cisco CallManager System Guide* Time Schedule Configuration, *Cisco CallManager Administration Guide* Time Period Configuration, *Cisco CallManager Administration Guide*
Step 3	If you want automatic call answering for other group call pickup, enable the Auto Call Pickup Enabled service parameter by entering the value True. The default specifies False.	Auto Call Pickup, page 10-2. Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 4	If the Auto Call Pickup Enabled service parameter is false, enter a value for the Call Pickup No Answer Timer service parameter. This parameter controls the amount of time that a call takes to get restored if a call is picked up by other group call pickup.	Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 5	Enter a value for the service parameter Pickup Locating Timer. This parameter controls the time for call selection for call pickup, group call pickup and other group call pickup.	Service Parameters Configuration, *Cisco CallManager Administration Guide*

Table 10-2 Other Group Call Pickup Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 6	To configure the Other Group Pickup (oPickup) softkey for the phone, modify and add the Standard User or Standard Feature softkey template to the phone. Modify the template to include the oPickup softkey with the following steps. • Choose **Device** > **Device Settings** > **Softkey Template** in Cisco CallManager Administration. • Choose the desired softkey template. • Choose the Softkey Layout Configuration link. • Choose On Hook or Off Hook call states. • Choose oPickup in the Unselected Softkeys box. Click the right arrow to move the oPickup softkey to the Selected Softkeys box. **Note** To restrict calls to be picked up by phones within its own group only, deny the oPickup softkey in the softkey template.	Assigning Softkey Templates to IP Phones, *Cisco CallManager Administration Guide*
Step 7	Notify users that the Call Pickup Group feature is available.	Refer to the phone documentation for instructions on how users access the Call Pickup feature on their Cisco IP Phone.

Additional Information

See the "Related Topics" section on page 10-15.

Setting the Service Parameters for Call Pickup Group

Cisco CallManager provides three clusterwide service parameters for call pickup group: Auto Call Pickup Enabled, Call Pickup Locating Timer, and Call Pickup No Answer Timer. Each service parameter includes a default and requires no special configuration.

- Auto Call Pickup Enabled—Default specifies False. This parameter determines whether the auto call pickup feature is enabled. To enable this capability, set the field to True.
- Call Pickup Locating Timer—Default specifies 1 second. This service parameter specifies the maximum time, in seconds, for a pickup to wait in order to get all alerting calls in the pickup groups from all of the nodes in the cluster.
- Call Pickup No Answer Timer—Default specifies 12 seconds. This parameter specifies the maximum time, in seconds, to wait before restoring the original call if a user, who initiates a pickup request, decides not to pick up the call. This is a required field.

Note To set the timers, choose **System > Service Parameters**, choose the Advanced icon or click the Advanced button, and update the fields in the **Clusterwide Parameters (Feature-Call Pickup)** pane.

Additional Information

See the "Related Topics" section on page 10-15.

Finding a Call Pickup Group

Because you may have several call pickup groups in your network, Cisco CallManager lets you locate call pickup groups on the basis of specific criteria. Use the following procedure to locate call pickup groups.

Note During your work in a browser session, Cisco CallManager Administration retains your call pickup group search preferences. If you navigate to other menu items and return to this menu item, Cisco CallManager Administration retains your call pickup group search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Call Pickup Group**.

The Find and List Call Pickup Groups window displays. Use the two drop-down list boxes to search for a call pickup group.

Step 2 From the first Find call pickup group where drop-down list box, choose one of the following criteria:

- Call Pickup Group Number
- Call Pickup Group Name
- Partition

From the second Find call pickup group where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

Tip To find all call pickup groups that are registered in the database, click **Find** without entering any search text.

A list of discovered call pickup groups displays with the following information:

- Call Pickup Group Name
- Call Pickup Group Number
- Partition

A Copy icon also appears on the display for duplicating information on any call pickup group.

Note You can delete multiple call pickup groups from the Find and List Call Pickup Group window by checking the check boxes next to the appropriate call pickup groups and clicking **Delete Selected**. You cannot delete call pickup groups that are assigned to directory numbers and lines.

Step 4 From the list of records, click the call pickup group name that matches your search criteria.

The window displays the call pickup group that you choose.

Additional Information

See the "Related Topics" section on page 10-15.

Configuring a Call Pickup Group

This section describes how to add, copy, and update a single call pickup group.

Procedure

Step 1 Choose **Call Routing** > **Call Pickup Group**.

Step 2 Perform one of the following tasks:

- To add a new Call Pickup Group, click **Add New**.
- To copy a Call Pickup Group, use the procedure in the "Finding a Call Pickup Group" section on page 10-10 to locate the call pickup group. Click the Copy icon.
- To update a Call Pickup Group, use the procedure in the "Finding a Call Pickup Group" section on page 10-10 to locate the call pickup group.

The Call Pickup Group Configuration window displays.

Step 3 Enter or update the appropriate settings as described in Table 10-1.

Step 4 To save the new or changed call pickup groups in the database, click **Save**.

Additional Information

See the "Related Topics" section on page 10-15.

Call Pickup Group Configuration Settings

Table 10-3 describes the call pickup group configuration settings. For related procedures, see the "Related Topics" section on page 10-15.

Table 10-3 Pickup Group Configuration Settings

Field	Description
Pickup Group Information	
Pickup Group Name	Enter up to 30 alphanumeric characters. For example, Operations. The pickup group name associates with the pickup group number. You can choose a pickup group by the pickup group name.
Pickup Group Number	Enter a unique directory number (integers) for the call pickup group that you want to add.
Partition	If you want to use a partition to restrict access to the call pickup group, choose the desired partition from the drop-down list box. If you do not want to restrict access to the call pickup group, choose <None> for the partition. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (**...**) displays next to the drop-down list box. Click the **...** button to display the Select Partition window. Enter a partial partition name in the **List items where Name contains** field. Click the desired partition name in the list of partitions that displays in the **Select item to use** box and click **OK**. **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose **CCMAdmin Parameters**. **Note** Make sure that the combination of call pickup group number and partition is unique within the Cisco CallManager cluster.
Associated Call Pickup Group Information—Find Pickup Numbers by Numbers/Partition	
Partition	See the preceding description of Partition in Pickup Group Information in this table.
Call Pickup Group Numbers Contain	Enter the DN or part of the DN of the pickup group that you want to find; then, click **Find**.
Available Call Pickup Groups	To add a member to the Associated Call Pickup Group list in the Current Associated Call Pickup Groups Information area, choose a Call Pickup Group from this list; then, click **Add to Associated Call Pickup Groups**.

Table 10-3 Pickup Group Configuration Settings (continued)

Field	Description
Current Associated Call Pickup Groups	
Selected Call Pickup Groups	To change order of the Call Pickup Groups listings, use the Up and Down arrows on the right side of this box to move the listings. Click **Reverse Order of Selected Numbers** to reverse the order of the listings. Use the Up and Down arrows below this box to move a call pickup group from this box to the Removed Call Pickup Groups box.
Removed Call Pickup Groups	Use the Up and Down arrows above this box to move a call pickup group from this box to the Selected Call Pickup Groups box.

Deleting a Call Pickup Group

This section describes how to delete a call pickup group from the Cisco CallManager database.

Before You Begin

You cannot delete a call pickup group number that is assigned to a line or directory number. To see a list of the directory numbers that are using this call pickup group, click the **Dependency Records** link. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about Dependency Records, see the "Accessing Dependency Records" section in the *Cisco CallManager Administration Guide*. To enable call pickup again for those directory numbers, you must reassign each of them to a new call pickup group. For details, see the "Assigning A Call Pickup Group to Directory Numbers" section on page 10-14.

Procedure

Step 1 Locate the call pickup group by using the procedure in the "Finding a Call Pickup Group" section on page 10-10.

Step 2 Click the call pickup group that you want to delete.

Step 3 Click **Delete**.

The call pickup group no longer displays in the Call Pickup Group Find/List window.

Additional Information

See the "Related Topics" section on page 10-15.

Defining a Pickup Group for Other Group Call Pickup

This section describes how to associate a call pickup group to your group for answering incoming calls for this associated group. You can associate up to ten call pickup groups with your group. The priority of answering calls for the associated groups goes from the first associated group to the last associated group on the associated group list. You can organize the list in the Call Pickup Group Configuration window as described in Table 10-1.

Procedure

Step 1 Locate your group by using the procedure in the "Finding a Call Pickup Group" section on page 10-10.

Step 2 In the Call Pickup Group Configuration window, scroll down to the Associated Call Pickup Group Information area.

Step 3 Enter information in the appropriate fields as described in Table 10-1.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 10-15.

Assigning A Call Pickup Group to Directory Numbers

This section describes how to assign a call pickup group to a directory number. Only directory numbers that are assigned to a call pickup group can use call pickup, group call pickup, and other group call pickup.

Before You Begin

Before you can assign a call pickup group to a directory number, you must create the call pickup group as described in the "Configuring a Call Pickup Group" section on page 10-11.

Procedure

Step 1 Choose **Device** > **Phone** or **Call Routing** > **Directory Number**.

Step 2 Enter the appropriate search criteria to find the phone or directory number that you want to assign to a call pickup group and click **Find**.

A list of phones or directory numbers that match the search criteria displays.

Step 3 Choose the phone or directory number to which you want to assign a call pickup group.

Step 4 If you are using the Directory Number Configuration window, proceed to Step 6.

Step 5 From the Association Information list on the Phone Configuration window, choose the directory number to which the call pickup group will be assigned.

Step 6 From the Call Pickup Group drop-down list box that displays in the Call Forward and Call Pickup Settings area, choose the desired call pickup group.

Step 7 To save the changes in the database, click **Save**.

Additional Information

See the "Related Topics" section on page 10-15.

Related Topics

- Call Pickup Group, page 10-1
- Finding a Call Pickup Group, page 10-10
- Configuring a Call Pickup Group, page 10-11
- Call Pickup Group Configuration Settings, page 10-12
- Deleting a Call Pickup Group, page 10-13
- Defining a Pickup Group for Other Group Call Pickup, page 10-13
- Assigning A Call Pickup Group to Directory Numbers, page 10-14
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Partition Configuration, *Cisco CallManager Administration Guide*
- Route Plan Report, *Cisco CallManager Administration Guide*
- Time-of-Day Routing, *Cisco CallManager System Guide*
- Softkey Template Configuration, *Cisco CallManager Administration Guide*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- Cisco IP Phone user documentation and release notes (all models)

Immediate Divert

The Immediate Divert feature allows you to immediately divert a call to a voice-messaging system. When the call gets diverted, the line becomes available to make or receive new calls.

Although Immediate Divert is not available to CTI applications, the CTI feature Transfer to Voicemail performs the same function as Immediate Divert but performs the function for CTI applications that third-party developers develop.

Access the Immediate Divert feature by using the iDivert softkey. Configure this softkey by using the Softkey Template Configuration window of Cisco CallManager Administration. The softkey template gets assigned to phones that are in the Cisco CallManager system.

This chapter provides the following information about Immediate Divert:

- Introducing Immediate Divert, page 11-1
- System Requirements for Immediate Divert, page 11-2
- Interactions and Restrictions, page 11-5
- Installing and Activating Immediate Divert, page 11-7
- Configuring Immediate Divert, page 11-7
- Setting the Service Parameter for Immediate Divert, page 11-8
- Related Topics, page 11-8

Introducing Immediate Divert

You will find that Immediate Divert, a Cisco CallManager supplementary service, is available for general use within the system. Immediate Divert does not require the user to log in to make the iDivert softkey available on the phone.

The call that is being diverted can be in the call offering, call on hold, or call active state. The call can be incoming or outgoing. The person on the call that is being diverted will receive the greeting of the voice-messaging system of the person who diverted the call.

Immediate Divert coexists with the Transfer to Voicemail feature.

System Requirements for Immediate Divert

Immediate Divert requires the following software component to operate:

- Cisco CallManager 5.0

The following SCCP and SIP phones support Immediate Divert by using the iDivert softkey that is configured in any Cisco CallManager softkey template:

- Cisco IP Phones (Models 7905, 7911, 7912, 7920, 7940, 7941, 7960, 7961, 7970, 7971)

The following voice-messaging systems support Immediate Divert:

- Voice-messaging systems such as Unity that use the skinny protocol
- Voice-messaging systems such as Octel that use SMDI

Call-Processing Requirements for Immediate Divert

The following sections describe call-processing requirements for Immediate Divert:

- Softkey Requirements, page 11-2
- Incoming Calls Requirements, page 11-2
- Outgoing Calls Requirements, page 11-3

Softkey Requirements

Because the iDivert softkey does not automatically get configured in a softkey template, use the Softkey Template Configuration window in Cisco CallManager Administration to configure the iDivert softkey in any available softkey template. You can configure the iDivert softkey in the following call states:

- On hook
- Connected
- On hold
- Ring in

Note The ring-in state in the softkey template represents the call-offering state in the phone call state.

Use the Phone Configuration window in Cisco CallManager Administration to assign the softkey template that contains the iDivert softkey to a phone.

For information about softkey template configuration, see Softkey Template Configuration in the *Cisco CallManager Administration Guide*. For information about assigning softkey templates to phones, see Cisco IP Phone Configuration in the *Cisco CallManager Administration Guide*.

Incoming Calls Requirements

The following list gives called party types in the call-forwarding chain that Immediate Divert supports:

- Party A calls party B.
- Party B forwards to party C.
- Party C forwards to party D.

Party B represents the original called party. Party C represents the last redirecting party. Party D represents the last called party.

Immediate Divert supports the following incoming call states:

- Call offering
- Call on hold
- Call active

A voice-messaging profile can represent either a specified voice-messaging profile or a default voice-messaging profile. (Choose default voice-messaging profiles by choosing None in the Voice Messaging Profile drop-down list box in the Directory Number Configuration window.)

A voice-messaging pilot in the voice-messaging profile identifies the voice-messaging system to which redirected calls go. The combination of a directory number and voice-messaging mask defines the voice-messaging mail box.

For information about voice messaging, see Cisco Voice-Mail Pilot Configuration and Voice-Mail Profile Configuration in the *Cisco CallManager Administration Guide*, and Voice Mail Connectivity to Cisco CallManager in the *Cisco CallManager System Guide*.

Outgoing Calls Requirements

Immediate Divert supports the following outgoing call states:

- Call on hold
- Call active

When the calling party presses the iDivert softkey, Immediate Divert redirects an outgoing call to a voice-messaging mail box that is specified in the voice-messaging profile that is associated with the calling party, regardless of the voice-messaging profiles of the original or last called parties.

For information about voice messaging, see Cisco Voice-Mail Pilot Configuration and Voice-Mail Profile Configuration in the *Cisco CallManager Administration Guide*, and Voice Mail Connectivity to Cisco CallManager in the *Cisco CallManager System Guide*.

Immediate Divert Phone Display Messages

Immediate Divert displays the following messages on the IP phone to indicate the status of an immediate divert action:

- Key is not active—The voice-messaging profile of the user who pressed iDivert does not have a voice-messaging pilot.
- Temporary failure—The voice-messaging system does not work, or a network problem exists.
- Busy—The voice-messaging system is busy.

Using Immediate Divert

The following scenarios provide examples of using the Immediate Divert feature.

Called Party Presses iDivert Softkey

1. Party A calls Manager A.
2. Manager A presses the iDivert softkey (call-offering state).
3. Immediate Divert diverts the call to Manager A voice-messaging mail box.
4. Party A receives the voice-messaging mail box greeting of Manager A.

Voice-Messaging Profile of an Original Called Party Does Not Have Voice-Messaging Pilot

1. Party A calls Party B.
2. The call gets forwarded to the personal line of Assistant B.
3. Assistant B presses the iDivert softkey (call-offering state).
4. Immediate Divert diverts the call to Assistant B voice-messaging mail box. Party B does not have a voice-messaging pilot number configured, but Assistant B does.
5. Party A receives the voice-messaging mail box greeting of Assistant B.

Manager A Forwards a Call to Manager B

1. Party A calls Manager A.
2. Manager A has line forwarded to Manager B.
3. Manager B presses the iDivert softkey (call-offering state).
4. Immediate Divert diverts the call to Manager B voice-messaging mail box because Manager B line associates with a default voice-messaging profile with a voice-messaging pilot and the last called party.
5. Party A receives the voice-messaging mail box greeting of Manager B.

Voice-Messaging Port Defined in a Voice-Messaging Profile is Busy

1. Party A calls Party B.
2. Party B presses the iDivert softkey (call offering state).
3. Immediate Divert cannot divert the call to the voice-messaging mail box because the voice-messaging port is busy.
4. Party B sees the message Busy on the IP phone.
5. The original call remains in the call-offering state.

Calling Party Calls a Call Center That Uses a Hunt Pilot Number

1. Party A calls Hunt List A.
2. Hunt List A member presses the iDivert softkey (call offering state).
3. Immediate Divert cannot divert the call to the voice-messaging mail box because Hunt List A does not have a voice-messaging profile.
4. Hunt List A member sees the message Key is Not Active on the IP phone.

Calling Party B Transfers a Call to Party C on Different Cisco CallManager Cluster

1. Party A calls Party B.
2. Party B transfers the call to Party C on a different Cisco CallManager cluster.
3. Party C answers the incoming call.
4. Party C presses the iDivert softkey.
5. Party A receives the voice-messaging mail box greeting of Party C.

Interactions and Restrictions

The following sections describe the interactions and restrictions for Immediate Divert:

- Interactions, page 11-5
- Restrictions, page 11-6

Interactions

The following sections describe how Immediate Divert interacts with Cisco CallManager applications and call processing:

- Multilevel Precedence and Preemption (MLPP), page 11-5
- Setting the Service Parameters for Call Park, page 9-7
- Call Forward, page 11-5
- Call Detail Records (CDR), page 11-6
- Conference, page 11-6
- Hunt List, page 11-6

Multilevel Precedence and Preemption (MLPP)

The following interactions occur between Immediate Divert and MLPP:

- Immediate Divert diverts calls to voice-messaging mail boxes regardless of the type of call (for example, a precedence call).
- When Alternate Party Diversion (call precedence) is activated, Call Forward No Answer (CFNA) also gets deactivated.

Call Forward

When the Forward No Answer setting on the Directory Number Configuration window is not configured, call forward uses the clusterwide CFNA timer service parameter, Forward No Answer Timer. If a user presses the iDivert softkey at the same time as the call is being forwarded, the call gets diverted to an assigned call forward directory number (because the timer was too short), not the voice-messaging mail box. To solve this situation, set the CFNA timer service parameter to a sufficient time (for example, 60 seconds).

Call Detail Records (CDR)

One CDR gets created for each iDivert invocation. Immediate Divert uses the text "Immediate Divert" for the "Onbehalf of" field in CDR.

Conference

When a conference participant presses the iDivert softkey, the remaining conference participants receive the voice-messaging mail box greeting of the Immediate Divert initiator. Conference types include Ad Hoc, Meet-Me, Barge, cBarge, and Join.

Hunt List

When you use a phone that is part of a line group in a hunt list and it has the iDivert softkey assigned to it, the system grays out the iDivert softkey and makes it not available when the phone receives a call from within the hunt list.

When the phone receives a call that is not associated with a hunt list, the iDivert softkey displays on the phone.

Restrictions

The following restrictions apply to Immediate Divert:

- Immediate Divert does not support QSIG devices (MGCP PRI QSIG T1 gateways and MGCP PRI QSIG E1 gateways).
- When Call Forward All (CFA) and Call Forward Busy (CFB) are activated, the system does not support Immediate Divert (CFA and CFB have precedence over Immediate Divert).
- Immediate Divert cannot divert a call to a busy voice-messaging port; however, voice-messaging ports can be members of a route/hunt list, thus reducing the busy port scenario.
- A member of a hunt list cannot invoke the iDivert softkey for a direct call because a hunt list does not have a voice-messaging profile. The message, Key is Not Active, displays on the IP phone.
- When Cisco CallManager goes down, users cannot receive voice messages unless a media path was established between a redirected party and the voice-messaging system before the Cisco CallManager went down.
- System does not support using Malicious Caller ID and Immediate Divert together.
- CTI applications do not have Immediate Divert available (applications use Transfer to Voicemail).
- Use the Call Park Display Timer service parameter to control the timer for the Immediate Divert text display on the IP phones. When the service parameter gets changed, the text display timer for Immediate Divert also gets changed.
- See the "Multilevel Precedence and Preemption (MLPP)" section on page 11-5 for restrictions about using MLPP.
- A race condition in connection with the Forward No Answer Timeout exists when the iDivert softkey gets pressed. For example, if a manager presses the iDivert softkey right after the Forward No Answer timeout, call forward will forward the call to a preconfigured directory number. However, if the manager presses the iDivert softkey before the Forward No Answer timeout, Immediate Divert diverts the call to the voice-messaging mail box of the manager.

- The calling and called parties can divert the call to their voice-messaging mail boxes if both take turns pressing the iDivert softkey. The voice-messaging mail box of the calling party would contain a portion of the outgoing greeting of the called party. Similarly, the voice-messaging mail box of the called party would contain a portion of the outgoing greeting of the calling party.
- When one participant in a conference presses the iDivert softkey, all remaining participants will receive an outgoing greeting of the participant who pressed iDivert. Conference types include Meet-Me, Ad Hoc, cBarge and Join.

Installing and Activating Immediate Divert

Immediate Divert, a system feature, comes standard with Cisco CallManager software. Immediate Divert does not require special installation.

Configuring Immediate Divert

This section contains the following information:

- Immediate Divert Configuration Checklist, page 11-7
- Setting the Service Parameter for Immediate Divert, page 11-8

Immediate Divert Configuration Checklist

Table 11-1 provides a checklist to configure Immediate Divert.

Table 11-1 Immediate Divert Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Change the Call Park Display Timer if the default is not appropriate.	Setting the Service Parameter for Immediate Divert, page 11-8
Step 2	Using the Directory Number Configuration window, associate a voice-mail profile to each user who will have access to Immediate Divert. **Note** This step assumes that voice-mail profiles and pilots are configured. See Configuring a Voice-Mail Profile and Configuring the Voice-Mail Pilot Number.	Configuring a Directory Number, *Cisco CallManager Administration Guide*
Step 3	Assign the iDivert softkey to the Standard User or Standard Feature softkey template. Assign the softkey in the On Hook, Connected, On Hold, and Ring In states.	Softkey Template Configuration, *Cisco CallManager Administration Guide*

Table 11-1 Immediate Divert Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 4	Using the Phone Configuration window, assign the Standard User or Standard Feature softkey template, to which you added the iDivert softkey, to each device that has Immediate Divert access. **Tip** To make the iDivert softkey available to many users, configure a softkey template with the iDivert softkey; then, assign that softkey template to a device pool and, finally, assign that device pool to all users who need iDivert.	Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*
Step 5	Notify users that the Immediate Divert feature is available.	Refer to the phone documentation for instructions on how users access Immediate Divert on their Cisco IP Phone.

Setting the Service Parameter for Immediate Divert

Immediate Divert uses the Cisco CallManager clusterwide service parameter Call Park Display Timer. The default for this service parameter specifies 10 seconds. Use the Call Park Display Timer service parameter to control the timer for the Immediate Divert text display on the IP phones. When the service parameter gets changed, the text display timer for Immediate Divert also gets changed. Set this timer for each server in a cluster that has the Cisco CallManager service and Immediate Divert configured.

For information about text displays, see the "Immediate Divert Phone Display Messages" section on page 11-3.

Where to Find More Information

Additional Cisco Documentation

- Cisco IP Phone administration documentation for Cisco CallManager
- Cisco IP Phone user documentation

Additional Information

See the "Related Topics" section on page 11-8.

Related Topics

- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Softkey Template Configuration, *Cisco CallManager Administration Guide*
- Cisco Voice-Mail Pilot Configuration, *Cisco CallManager Administration Guide*
- Voice-Mail Profile Configuration, *Cisco CallManager Administration Guide*
- Voice Mail Connectivity to Cisco CallManager, *Cisco CallManager System Guide*

CHAPTER 12

Malicious Call Identification

The Malicious Call Identification (MCID) supplementary service allows you to report a call of a malicious nature by requesting that Cisco CallManager identify and register the source of an incoming call in the network.

This chapter provides the following information about the Malicious Call Identification feature:

- Introducing Malicious Call Identification, page 12-1
- System Requirements for Malicious Call ID, page 12-2
- Interactions and Restrictions, page 12-2
- Installing Malicious Call ID, page 12-4
- Configuring Malicious Call ID, page 12-4
- Troubleshooting Malicious Call ID, page 12-8
- Related Topics, page 12-8

Introducing Malicious Call Identification

Malicious Call Identification (MCID), an internetwork service, allows users to initiate a sequence of events when they receive calls with a malicious intent. The user who receives a disturbing call can invoke the MCID feature by using a softkey or feature code while connected to the call. The MCID service immediately flags the call as a malicious call with an alarm notification to the Cisco CallManager administrator. The MCID service flags the call detail record (CDR) with the MCID notice and sends a notification to the off-net PSTN that a malicious call is in progress.

The system supports the MCID service, which is an ISDN PRI service, when using PRI connections to the PSTN. The MCID service includes two components:

- MCID-O—An originating component that invokes the feature upon the user's request and sends the invocation request to the connected network.
- MCID-T—A terminating component that receives the invocation request from the connected network and responds with a success or failure message that indicates whether the service can be performed.

Note Cisco CallManager supports only the originating component at this time.

Using the Malicious Call ID Feature with Cisco CallManager

The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives this type of call, the Cisco CallManager system administrator can assign a new softkey template that adds the Malicious Call softkey to the user's phone. For POTS phones that are connected to a SCCP gateway, users can use a hookflash and enter a feature code of *39 to invoke the MCID feature.

When the MCID feature is used, the following actions take place:

1. The user receives a threatening call and presses the Malicious Call softkey (or enters the feature code *39).
2. Cisco CallManager sends the user a confirmation tone if the device can play a tone—and a text message on a phone that has a display—to acknowledge receiving the MCID notification.
3. Cisco CallManager updates the CDR for the call with an indication that the call is registered as a malicious call.
4. Cisco CallManager generates the alarm and local syslogs entry that has the event information.
5. Cisco CallManager sends a MCID invocation through the facility message to the connected network. The facility information element (IE) encodes the MCID invocation.
6. After receiving this notification, the PSTN or other connected network can take actions, such as providing legal authorities with the call information.

System Requirements for Malicious Call ID

Malicious Call ID service requires Cisco CallManager 5.0 to operate.

The following gateways and connections support MCID service:

- PRI gateways that use the MGCP PRI backhaul interface for T1 (NI2) and E1 (ETSI) connections
- H.323 trunks and gateways

The Cisco SIP and SCCP IP Phones support MCID by using the Malicious Call Trace softkey in the Standard User softkey template.

The Cisco ATA 186 analog phone ports support MCID by using the feature code (*39).

Interactions and Restrictions

The following sections describe the interactions and restrictions for Malicious Call Identification.

- Interactions, page 12-2
- Restrictions, page 12-4

Interactions

The following sections describe how Malicious Call Identification interacts with Cisco CallManager applications and call processing:

- Conference Calls, page 12-3
- Extension Mobility, page 12-3

- Call Detail Records, page 12-3
- Alarms, page 12-3

Conference Calls

When a user is connected to a conference, the user can use the MCID feature to flag the call as a malicious call. Cisco CallManager sends the MCID indication to the user, generates the alarm, and updates the CDR. However, Cisco CallManager does not send an MCID invoke message to the connected network that might be involved in the conference.

Extension Mobility

Extension mobility users can have the MCID softkey as part of their user device profile and can use this feature when they are logged on to a phone.

Call Detail Records

To track malicious calls by using CDR, you must set the CDR Enabled Flag to True in the Cisco CallManager service parameter. When the MCID feature is used during a call, the CDR for the call contains "CallFlag=MALICIOUS" in the Comment field.

Alarms

To record alarms for the MCID feature in the Local Syslogs, you must configure alarms in Cisco CallManager Serviceability. Under Local Syslogs, enable alarms for the "Informational" alarm event level.

When the MCID featured is used during a call, the system logs an SDL trace and a Cisco CallManager trace in alarms. You can view the Alarm Event Log by using Cisco CallManager Serviceability. The traces provide the following information:

- Date and time
- Type of event: Information
- Information: Malicious Call Identification feature gets invoked in Cisco CallManager
- Called Party Number
- Called Device Name
- Called Display Name
- Calling Party Number
- Calling Device Name
- Calling Display Name
- Application ID
- Cluster ID
- Node ID

Refer to the *Cisco CallManager Serviceability Administration Guide* for more information about alarms and traces.

Restrictions

The following restrictions apply to Malicious Call Identification:

- Cisco CallManager supports only the malicious call identification originating function (MCID-O). Cisco CallManager does not support the malicious call identification terminating function (MCID-T). If Cisco CallManager receives a notification from the network of a malicious call identification, Cisco CallManager ignores the notification.
- MCID does not work across intercluster trunks because Cisco CallManager does not support the MCID-T function.
- Cisco MGCP FXS gateways do not support MCID. No mechanism exists for accepting the hookflash and collecting the feature code in MGCP.
- MCID does not work over QSIG trunks because MCID is not a QSIG standard.
- The Cisco VG248 Analog Phone Gateway does not support MCID.
- Skinny Client Control Protocol (SCCP) IP phones use a softkey to invoke the MCID feature.

See the"Configuring Malicious Call ID" section on page 12-4 for configuration details.

Installing Malicious Call ID

Malicious Call Identification, which is a system feature, comes standard with Cisco CallManager software. MCID does not require special installation or activation.

Configuring Malicious Call ID

This section contains the following information:

- Malicious Call ID Configuration Checklist, page 12-4
- Setting the Service Parameter for Malicious Call ID, page 12-5
- Configuring Alarms for Malicious Call ID, page 12-6
- Adding a Softkey Template for Malicious Call ID, page 12-6
- Giving the Malicious Call Identification Feature to Users, page 12-7
- Removing the Malicious Call Identification Feature from a User, page 12-7

Malicious Call ID Configuration Checklist

Table 12-1 provides a checklist for configuring Malicious Call Identification. You must configure the softkey template and assign the template to an IP phone to make the feature available to IP phones.

Table 12-1 MCID Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure the CDR service parameter.	Setting the Service Parameter for Malicious Call ID, page 12-5 Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 2	Configure the alarm.	Configuring Alarms for Malicious Call ID, page 12-6 *Cisco CallManager Serviceability Administration Guide*
Step 3	Configure a softkey template with the Malicious Call Trace softkey.	Adding a Softkey Template for Malicious Call ID, page 12-6 Softkey Template Configuration, *Cisco CallManager Administration Guide*
Step 4	Assign the MCID softkey template to an IP phone.	Giving the Malicious Call Identification Feature to Users, page 12-7 Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
Step 5	Notify users that the Malicious Call Identification feature is available.	Refer to the phone documentation for instructions on how users access the Malicious Call Identification feature on their Cisco IP Phone.

Setting the Service Parameter for Malicious Call ID

To enable Cisco CallManager to flag a CDR with the MCID indicator, you must enable the CDR flag. Use the following procedure in Cisco CallManager Administration to enable CDR.

Procedure

Step 1 From the CCM Administration window, choose **System** > **Service Parameters**.

Step 2 Choose the Cisco CallManager server name.

Step 3 In the Service field, choose **Cisco CallManager**. The Service Parameters Configuration window displays.

Step 4 In the System area, set the CDR Enabled Flag field to **True** if it is not already enabled.

Step 5 If you need to make the change, click **Save**.

Configuring Alarms for Malicious Call ID

To ensure that the MCID alarm information appears in the Local Syslogs, you need to enable the alarm event level. Use Cisco CallManager Serviceability and the following procedure to activate alarms for MCID.

Procedure

Step 1 From the Navigation drop-down list box, choose Serviceability and click **Go**. Cisco CallManager Serviceability displays.

Step 2 Choose **Alarm > Configuration**. The Alarm Configuration window displays.

Step 3 From the servers list, choose the Cisco CallManager server.

Step 4 In the Configured Services list box, choose **Cisco CallManager**. The Alarm Configuration window updates with configuration fields.

Step 5 Under Local Syslogs, in the Alarm Event Level drop-down list, choose **Informational**.

Step 6 Under Local Syslogs, check the **Enable Alarm** check box.

Step 7 If you want to enable the alarm for all nodes in the cluster, check the **Apply to All Nodes** check box.

Step 8 Click **Update** to turn on the informational alarm.

Additional Information

See the "Related Topics" section on page 12-8.

Adding a Softkey Template for Malicious Call ID

Use this procedure in Cisco CallManager Administration to add the Malicious Call softkey to a template.

Procedure

Step 1 From CCM Administration, choose **Device** > **Device Settings** > **Softkey Template**. The Find and List Softkey Templates window displays.

Step 2 Click the **Add New** button. The Softkey Template Configuration window displays.

Step 3 In the Create a softkey template based on field, choose **Standard User**.

Step 4 Click **Copy**. The Softkey Template Configuration window refreshes with new fields.

Step 5 In the Softkey Template Name field, enter a name that indicates that this is a MCID softkey template.

Step 6 In the Description field, enter a description that indicates that this is a MCID softkey template.

Step 7 Click **Save**. The Softkey Template Configuration window refreshes with additional configuration fields.

Step 8 Click the **Go** button that is next to the **Configure Softkey Layout** related links box. The Softkey Layout Configuration window displays.

Step 9 In the Select a call state to configure field, choose **Connected**. The list of Unselected Softkeys changes to display the available softkeys for this call state.

Step 10 In the Unselected Softkeys list, choose **Toggle Malicious Call Trace**.

Step 11 To move the softkey to the Selected keys list, click the right arrow.

Step 12 Click **Save** to ensure that the softkey template is configured.

Additional Information

See the "Related Topics" section on page 12-8.

Giving the Malicious Call Identification Feature to Users

To provide the Malicious Call Identification feature for users, you assign the MCID softkey template to their IP phone.

Note For users who do not have phones that can use a softkey, give them the feature code information and instructions on how to invoke the feature.

Procedure

Step 1 Choose **Device** > **Phone**. The Find and List Phones window displays.

Step 2 To locate the phone configuration, enter appropriate phone search information; click **Find**.

Step 3 Choose the phone that you want to update.

Step 4 Locate the Softkey Template field and choose the MCID softkey template that you created from the drop-down list.

Step 5 To save the changes in the database, click **Save**.

Step 6 To activate the changes on the phone, click **Reset**.

Step 7 Notify the user that the Malicious Call Identification feature is available.

Additional Information

See the "Related Topics" section on page 12-8.

Removing the Malicious Call Identification Feature from a User

To remove the Malicious Call Identification feature from users, you assign another softkey template to their IP phone.

Procedure

Step 1 Choose **Device** > **Phone**. The Find and List Phones window displays.

Step 2 To locate the phone configuration, enter appropriate phone search information and click **Find**.

Step 3 Choose the phone that you want to update.

Step 4 Locate the Softkey Template field and choose a softkey template without MCID from the drop-down list.

Step 5 To save the changes in the database, click **Save**.

Step 6 To activate the changes on the phone, click **Reset**.

Step 7 Notify the user that the Malicious Call Identification feature is no longer available.

Additional Information

See the "Related Topics" section on page 12-8.

Troubleshooting Malicious Call ID

To assist with tracking and troubleshooting the Malicious Call ID feature, the system makes Cisco CallManager SDL traces and alarms available.

For information about using these traces and alarms, refer to the *Cisco CallManager Serviceability Administration Guide*.

Additional Information

See the "Related Topics" section on page 12-8.

Related Topics

- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Softkey Template Configuration, *Cisco CallManager Administration Guide*
- Malicious Call ID Configuration Checklist, page 12-4
- Setting the Service Parameter for Malicious Call ID, page 12-5
- Adding a Softkey Template for Malicious Call ID, page 12-6
- Configuring Alarms for Malicious Call ID, page 12-6
- Giving the Malicious Call Identification Feature to Users, page 12-7
- Removing the Malicious Call Identification Feature from a User, page 12-7

Additional Cisco Documentation

- *Cisco CallManager Serviceability Administration Guide*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- Cisco IP Phone user documentation and release notes (all models)

CHAPTER 13

Multilevel Precedence and Preemption

The Multilevel Precedence and Preemption (MLPP) service allows properly validated users to place priority calls. If necessary, users can preempt lower priority phone calls.

Precedence designates the priority level that is associated with a call. Preemption designates the process of terminating lower precedence calls that are currently using the target device, so a call of higher precedence can be extended to or through the device.

An authenticated user can preempt calls either to targeted stations or through fully subscribed time-division-multiplexing (TDM) trunks. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations.

This chapter covers the following topics:

- Introducing MLPP, page 13-1
- Interactions and Restrictions, page 13-26
- Installing and Activating MLPP, page 13-28
- MLPP Configuration Checklist, page 13-28
- Setting the Enterprise Parameters for MLPP, page 13-29
- Related Topics, page 13-30

Introducing MLPP

The Multilevel Precedence and Preemption (MLPP) service allows placement of priority calls. Properly validated users can preempt lower priority phone calls with higher priority calls. An authenticated user can preempt calls either to targeted stations or through fully subscribed TDM trunks. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations.

The following topics describe the MLPP service:

- MLPP Terminology, page 13-2
- Precedence, page 13-3
- Executive Override Precedence Level, page 13-3
- Preemption, page 13-6
- Domain, page 13-6
- Location-Based MLPP, page 13-6

- MLPP Over Intercluster Trunks, page 13-7
- MLPP Precedence Patterns, page 13-7
- MLPP Indication Enabled, page 13-7
- Precedence Call Setup, page 13-8
- Alternate Party Diversion, page 13-9
- MLPP Preemption Enabled, page 13-10
- Preemption Details, page 13-11
- MLPP Announcements, page 13-16
- MLPP Numbering Plan Access Control for Precedence Patterns, page 13-19
- MLPP Trunk Selection, page 13-21
- MLPP Hierarchical Configuration, page 13-23
- Service Parameter Special Trace Configuration, page 13-23
- CDR Recording for Precedence Calls, page 13-24
- Line Feature Interaction, page 13-24
- Call Preservation, page 13-26
- Automated Alternate Routing, page 13-26
- MGCP and PRI Protocol, page 13-26
- Secure Endpoints and Secure Communications, page 13-26

MLPP Terminology

The following terms apply to the MLPP service:

- Call—A voice, video, or data connection between two or more users or network entities that is achieved by dialing digits or otherwise routing to a destination according to a predefined dialing plan.
- Precedence—Priority level that is associated with a call.
- Preemption—Process that terminates existing calls of lower precedence and extends a call of higher precedence to or through that target device.
- Precedence call—A call with precedence level that is higher than the lowest level of precedence.
- MLPP call—A call that has a precedence level established and is either being set up (that is, before alerting) or is set up.
- Active call—A call that has the connection established and the calling and called parties are active on the call.
- MLPP domain ID—Specifies the collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber that belongs to a particular domain places a precedence call to another MLPP subscriber that belongs to the same domain, MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. MLPP service availability does not go across different domains.
- MLPP Indication Enabled device—In Cisco CallManager, a device for which the device and Cisco CallManager support precedence and preemption signaling procedures in the device control protocol and that is configured as such in the Cisco CallManager system.

- MLPP Preemption Enabled device—In Cisco CallManager, a device for which the device and Cisco CallManager support preemption signaling procedures in the device control protocol and that is configured as such in the Cisco CallManager system. Cisco CallManager can initiate preemption on this interface.

Precedence

Precedence indicates the priority level that is associated with a call. Precedence assignment represents an ad hoc action in that the user may choose to apply or not to apply a precedence level to a call attempt. MLPP precedence does not relate to call admission control or enhanced emergency services (E911). Dedicated dial patterns in Cisco CallManager administration allow users to initiate an MLPP request. Configuration of the calling search space(s) (CSS) that is associated with the calling party (device, line, and so forth) controls a calling party's ability to dial a precedence pattern to attempt to originate a precedence call.

The Defense Switched Network (DSN) and the Defense Red Switched Network (DRSN) designate the target system for initial MLPP deployment. You generally can apply mechanisms for assigning precedence levels to calls, however, in Cisco CallManager Administration to any dial plan by defining precedence dial patterns and calling search spaces that allow or restrict access to these patterns. In the DSN, a dial plan gets defined such that a precedence call is requested by using the string prefix NP, where P specifies the requested precedence level and N specifies the preconfigured MLPP access digit. Precedence priorities are as follows.

- Executive Override
- Flash Override
- Flash
- Immediate
- Priority
- Routine

Without specific invocation of precedence, the system processes a call by using normal call processing and call forwarding.

When a user profile is assigned to a phone, either as a default assignment or through extension mobility, the phone inherits the configuration of the assigned user, including any CSS that is associated with the user. The phone CSS can, however, override the user profile. Cisco CallManager assigns the precedence level that is associated with the dialed pattern to the call when a pattern match occurs. The system sets the call request as a precedence call with the assigned precedence level.

When a precedence call is offered to a destination, Cisco CallManager provides precedence indications to the source and destination of a precedence call, respectively, if either is MLPP Indication Enabled. For the source, this indication comprises a precedence ringback tone and display of the precedence level/domain of the call, if the device supports display. For the destination, the indication comprises a precedence ringer and display of the precedence level/domain of the call, if the device supports display.

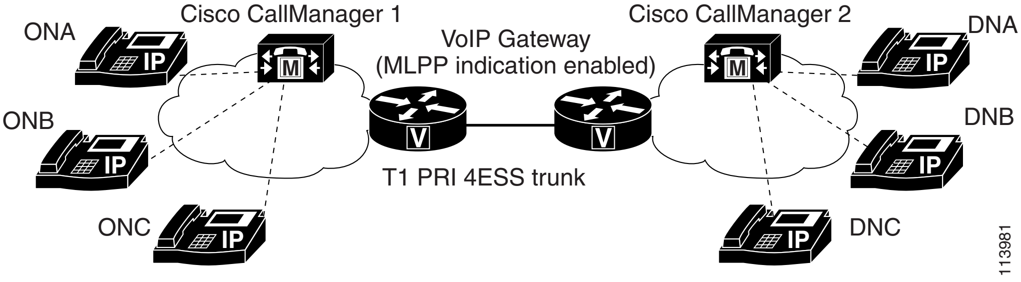
Executive Override Precedence Level

The highest precedence level specifies the Executive Override precedence level. When the Executive Override precedence level preempts a lower precedence call, the Executive Override call can change its precedence level to Flash Override (next highest level), so a subsequent Executive Override call can preempt the first precedence call.

Preempting an Executive Override precedence call requires that the Executive Override Call Preemptable service parameter be set to True. If the service parameter is set to False, an Executive Override precedence call keeps its precedence level and cannot be preempted.

Figure 13-1 shows an example of two Executive Override precedence calls, one that can be preempted, and one that cannot be preempted.

Figure 13-1 Executive Override Precedence Calls Example



In the example, in Cisco CallManager cluster 1, the Executive Override Call Preemptable service parameter specifies False, whereas in Cisco CallManager cluster 2, the Executive Override Call Preemptable service parameter specifies True.

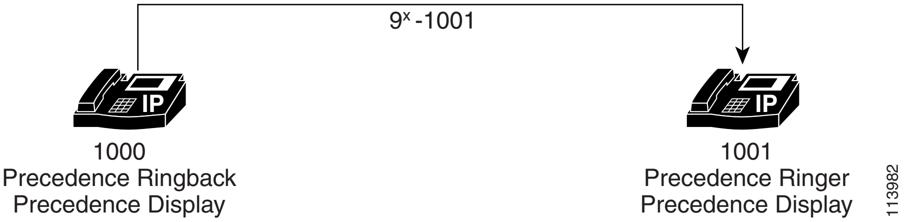
In the example, ONA makes an Executive Override precedence call to DNA from cluster 1 to cluster 2 through the T1 PRI 4ESS trunk. DNA answers, and the call connects.

In cluster 1, if ONB tries to call ONA by placing an Executive Override precedence call, ONB receives a Blocked Precedence Announcement (BPA) because Executive Override calls cannot be preempted in cluster 1. If ONB calls DNA by placing an Executive Override precedence call, the call between ONA and DNA gets preempted because Executive Override calls can be preempted in cluster 2. Likewise, if DNB calls DNA by placing an Executive Override precedence call, the subsequent Executive Override precedence call preempts the call between ONA and DNA.

Executive Override Precedence Call Setup

Figure 13-2 shows an example of the events that take place when an Executive Override precedence call gets placed.

Figure 13-2 Executive Override Precedence Call Setup



In the example, phone 1000 goes offhook and dials 9*1001. (Route pattern 9*XXXX setting specifies Executive Override.)

For the source, if this precedence call succeeds, Cisco CallManager signals Cisco IP Phone to play a ringback tone to the user. If Cisco IP Phone 1000 is MLPP Indication Enabled, precedence ringback tone plays. Otherwise, normal ringback tone plays.

If the precedence call cannot connect, a Blocked Precedence Announcement (BPA) plays if Cisco IP Phone 1000 is MLPP Indication Enabled. Otherwise, a normal reorder tone plays.

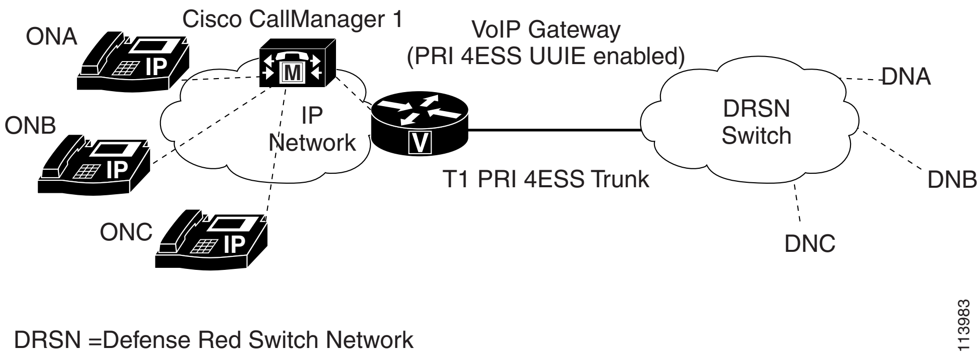
For the destination, if the Executive Override precedence call gets offered to Cisco IP Phone 1001 successfully, Cisco CallManager signals the destination to generate an audible ringer at the device. If Cisco IP Phone 1001 is MLPP Indication Enabled, a precedence ring plays. Otherwise, a normal ring plays.

Also, Cisco IP Phone 1001 displays precedence information (such as the Flash Override precedence call icon) if phone 1001 is MLPP Indication Enabled. Otherwise, no precedence information displays.

Executive Override Precedence Calls Across the PRI 4ESS Interface

Figure 13-3 shows an example of an Executive Override precedence call across the PRI 4ESS interface.

Figure 13-3 Executive Override Precedence Call Across the PRI 4ESS Interface



Cisco CallManager processes Executive Override precedence calls across the PRI 4ESS interface using the same method that it uses to process other precedence calls, except that the precedence level passes through PRI 4ESS UUIE.

The precedence information through UUIE gets passed only when UUIE Status on the service parameter window is True and Passing Precedence Through UUIE gets selected on the Gateway Configuration window.

PRI 4ES UUIE-Based MLPP Interface to DRSN

A previous release of Cisco CallManager offered MLPP for PRI interface that was developed according to the ANSI.619a specification to connect with Defense Switched Network (DSN) switches. Defense Red Switch Network (DRSN) switches do not support ANSI T1.619a-based MLPP but do support MLPP over the PRI 4ESS interface by using the UUIE. Cisco CallManager now supports passing the MLPP information through the PRI 4ESS UUIE field.

Preemption

The preemption process terminates lower precedence calls that are currently using the target device, so a call of higher precedence can be extended to or through the device. Preemption includes the notification and acknowledgement of preempted users and the reservation of shared resources immediately after preemption and prior to call termination. Preemption can take one of the following forms, depending on which method is invoked:

- User Access Channel Preemption—This type of preemption applies to phones and other end-user devices. In this type of preemption, if a called user access channel needs to be preempted, both the called party and the parties to which it is connected receive preemption notification, and the existing MLPP call gets cleared immediately. The called party must acknowledge the preemption before the higher precedence call completes. The called party then gets offered the new MLPP call. If the called party does not acknowledge the preemption, the higher precedence call does proceed after 30 seconds.
- Common Network Facility Preemption—This type of preemption applies to trunks. This type of preemption means that the network resource is busy with calls, some of which are of lower precedence than the call that the calling party requests. One or more of these lower precedence calls gets preempted to complete the higher precedence call.

Note Ensure that all devices that a call uses to preempt an existing call are preemption enabled. Because it is not sufficient for the calling and called devices (phone) to be preemption enable, ensure that the gateways that are used for the call also are preemption enabled.

Domain

The MLPP domain subscription of the originating user determines the domain of the call and its connections. Only higher precedence calls in one domain can preempt connections that calls in the same domain are using.

Administrators enter domains in Cisco CallManager Administration as hexadecimal values of zero or greater.

Additional Information

See the "Related Topics" section on page 13-30.

Location-Based MLPP

Cisco CallManager supports MLPP on Skinny Client Control Protocol phones and TDM (PRI/CAS) trunks. Cisco CallManager also supports MLPP on wide-area network (WAN) links. Location-based call admission control (CAC) manages WAN link bandwidth in Cisco CallManager. Enhanced locations take into account the precedence level of calls and preempt calls of lower precedence when necessary to accommodate higher precedence calls.

Enhancing locations mean that, when a precedence call arrives and not enough bandwidth can be found to connect the call to the destination location, Cisco CallManager finds the call or calls with the lowest precedence level and preempts the call(s) to make sufficient bandwidth available for a higher precedence call. If the bandwidth requirement still cannot be satisfied after going through the preemption procedure, the newly placed call fails.

Additional Information

See the "Related Topics" section on page 13-30.

MLPP Over Intercluster Trunks

Cisco CallManager supports MLPP precedence and preemption over intercluster trunks. Dialed digits communicate the precedence level. The location call admission control mechanism controls preemption. Announcements and MLPP cause codes also become available across intercluster trunks.

MLPP Precedence Patterns

To set up MLPP precedence patterns, access the Translation Pattern Configuration window in Cisco CallManager Administration where the following MLPP precedence patterns are available:

- Executive override (highest)
- Flash override
- Flash
- Immediate
- Priority
- Routine (lowest)
- Default (means precedence level does not get changed)

Refer to the Translation Pattern Configuration section in the *Cisco CallManager Administration Guide* for details.

MLPP Indication Enabled

MLPP indication-enabled devices include the following characteristics:

- MLPP indication-enabled devices can play preemption tones.
- MLPP indication-enabled devices can receive MLPP preemption announcements that the announcement server generates.
- MLPP indication-enabled devices can receive preemption.

To set up devices to enable MLPP indication, use the configuration window for each respective device. In the MLPP Indication field of each device, set the value to *On*.

Refer to the following topics for details of setting MLPP indication for devices:

- Device Pool Configuration, *Cisco CallManager Administration Guide*
- Gateway Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Device Profile Configuration, *Cisco CallManager Administration Guide*
- Default Device Profile Configuration, *Cisco CallManager Administration Guide*

Precedence Call Setup

The following sequence of events takes place during setup of a precedence call:

1. User goes off hook and dials a precedence call. The call pattern specifies NP-XXX, where N specifies the precedence access digit and P specifies the precedence level for the call.
2. The calling party receives the special precedence ringback and a precedence display while the call is processing.
3. The called party receives the special precedence ringer and a precedence display that indicates the precedence call.

Example

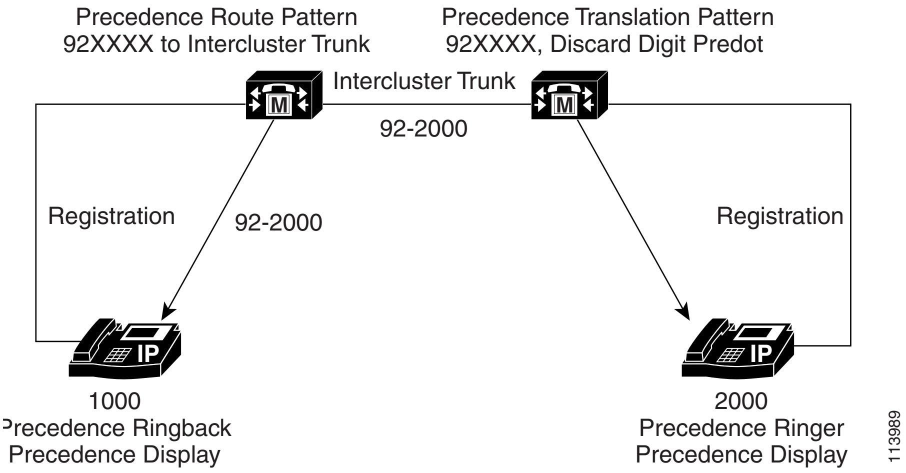
Party 1000 makes a precedence call to party 1001. To do so, party 1000 dials the precedence call pattern, such as 90-1001.

While the call processes, the calling party receives precedence ringback and precedence display on the calling Cisco IP Phone. After acknowledging the precedence call, the called party receives a precedence ringer (receives a special ring) and a precedence display on the called Cisco IP Phone.

Precedence Call Setup Across Intercluster Trunks

Figure 13-4 shows an example of a configuration that can be used to set up precedence calls over intercluster trunks. Because no precedence information element support exists over intercluster trunks, transmission of extra digits carries the precedence information. The dial plan must be set up appropriately on both clusters to accomplish transmission of the precedence information.

Figure 13-4 Precedence Call Setup Across Intercluster Trunks Example



In this example, 1000 dials 92-2000, which matches the appropriate precedence patterns on both clusters and sets up the precedence call.

Alternate Party Diversion

Alternate Party Diversion (APD) comprises a special type of call forwarding. If users are configured for APD, APD takes place when a precedence call is directed to a directory number (DN) that is busy or does not answer.

MLPP APD applies only to precedence calls. An MLPP APD call disables the DN Call Forward No Answer setting for precedence calls.

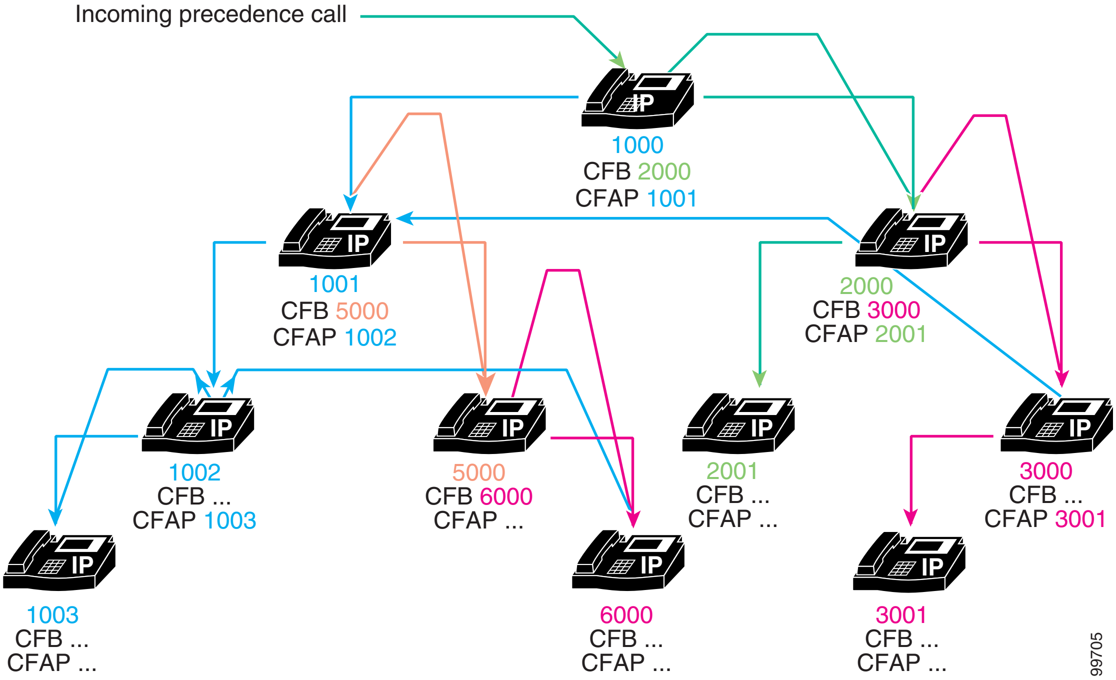
Precedence calls do not normally forward to voice-messaging system, as controlled by the value of the Use Standard VM Handling For Precedence Calls enterprise parameter. Refer to the "Setting the Enterprise Parameters for MLPP" section on page 13-29 for details.

To set up APD, the administrator configures the Multilevel Precedence and Preemption Alternate Party Settings on the Directory Number Configuration window of the DN that is the target of an MLPP precedence call. Refer to the Cisco IP Phone Configuration section of the *Cisco CallManager Administration Guide* for details.

Example

Figure 13-5 illustrates the Alternate Party Diversion that takes place when a called party receives a precedence call and the party is configured for Alternate Party Diversion.

Figure 13-5 Alternate Party Diversion Example



In the example, a calling party placed a precedence call to party 1000. Called party 1000 has a Call Forward Busy (CFB) setting of 2000 and a Call Forward Alternate Party (CFAP) setting of 1001. The figure shows the CFB and CFAP settings for all other parties in this example.

When 1000 receives a precedence call but is busy, the call routes to party 2000. If party 2000 is also busy, the call routes to party 3000. If neither party 2000 nor party 3000 answers the call, however, the call routes to party 1001. That is, the call routes to the alternate party that is designated for the originally called party, *not* to the alternate parties that are designated for the Call Forward Busy parties that are associated with the originally called party.

Likewise, if party 1001 is busy and does not answer the call, the call forwards to party 5000. If party 5000 is busy, the call forwards to party 6000. If neither party 5000 nor party 6000 answers the call, however, the call forwards to party 1001's alternate party destination, which is party 1002. If party 1002 is busy or does not answer, the call forwards to party 1003, which is party 1002's alternate party designation.

MLPP Preemption Enabled

Enable MLPP preemption by explicitly configuring preemption-capable devices for preemption.

Receiving Preemption

A device that is preemption disabled (by setting the MLPP Preemption value to *Disabled*) can still receive precedence calls in an MLPP network, but the device itself does not get preempted. The preemption-disabled device can be connected to a call that gets preempted (at another device), in which case, the device receives preemption.

Preemption Enabled

Enable devices for preemption by setting the device MLPP Preemption value to either *Forceful* or *Default*. If the device MLPP Preemption value is set to *Forceful*, the system can preempt the device at its own interface. That is, the device can get preempted when a precedence call contends for the device resources.

If the device MLPP Preemption setting is *Default*, the device inherits its MLPP Preemption setting from its device pool. If the device's device pool MLPP Preemption setting is *Forceful*, or if the device pool MLPP Preemption setting is also *Default* but the MLPP Preemption Setting enterprise parameter value is *Forceful Preemption*, the device inherits preemption enabling.

To set up devices to enable MLPP preemption, use the configuration window for each respective device. In the MLPP Preemption field of each device, set the value to *Forceful* or *Default*.

Refer to the following topics for details of setting MLPP preemption for devices:

- Device Pool Configuration, *Cisco CallManager Administration Guide*
- Gateway Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Device Profile Configuration, *Cisco CallManager Administration Guide*
- Default Device Profile Configuration, *Cisco CallManager Administration Guide*

Preemption Details

The following types of preemption exist:

- User Access Preemption
- Common Network Facility Preemption~~.~~
- Location-based Preemption

User Access Preemption

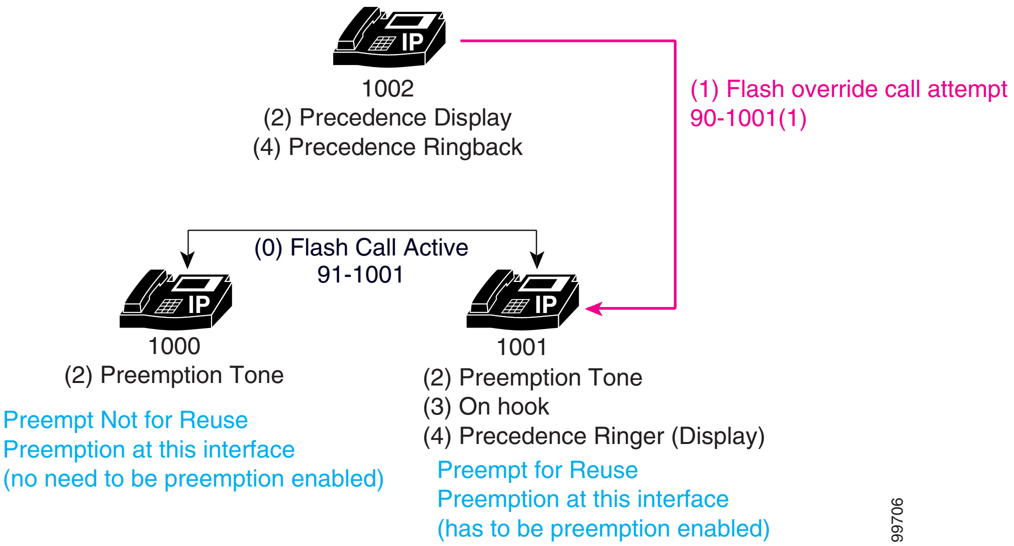
User access preemption takes place when a user places a precedence call to a user that is already active on a lower level precedence call. Both calls are in the same MLPP domain. You can use this type of preemption for MLPP Indication Enabled phones that the Cisco Skinny Client Control Protocol controls in the Cisco CallManager MLPP system. Preemption occurs if a precedence call request is validated and if the requested precedence of the call is greater than the precedence of an existing call that is connected at the destination MLPP Preemption Enabled phone. Call processing uses a preemption tone to notify the connected parties of the preemption and releases the active call. When the called party acknowledges the preemption by hanging up, the called party gets offered the new MLPP call.

To understand the sequence of steps that takes place during user access preemption, see the following example.

Example

Figure 13-6 illustrates an example of user access preemption.

Figure 13-6 User Access Preemption Example



In the example of user access preemption, the following sequence of events takes place:

1. User 1000 places a precedence call of precedence level flash override to user 1001, who answers the call. In this example, user 1000 dials 90-1001 to place the precedence call.
2. User 1002 places a precedence call to user 1001 by dialing 9*-1001. This call is of precedence level Executive Override which represents a higher precedence call than the active precedence call.

3. While the call is directed to user 1001, the calling party receives precedence display (that is, flash override display, not executive override display), and the parties involved in the existing lower precedence call both receive preemption tones.
4. To complete preemption, the parties involved in the lower precedence call (users 1000 and 1001) hang up.
5. The higher level precedence call gets offered to user 1001, who receives a precedence ringer. The calling party, user 1002, receives precedence ringback.

Distinct preemption types take place in this instance. For the party that is not the destination of the higher precedence call, Preemption Not for Reuse takes place. Because preemption is not taking place at this interface, this device does not need to be preemption enabled. For the party that is the destination of the higher precedence call, Preemption for Reuse takes place. Because preemption does take place at this interface, ensure that this device is preemption enabled.

User Access Channel Nonpreemptable

You can configure an end-user device as MLPP Indication Enabled but not MLPP Preemption Enabled. In this case, a phone that can generate MLPP indications (using special preemption tones and ringers) does not have preemption procedures supported in its device control protocol in Cisco CallManager. The administrator can also disable preemption procedures for a phone even though Cisco CallManager Administration supports the procedures.

Historically, user access devices (phones) have limited or no mechanisms for handling multiple, simultaneous calls. Even with the Call Waiting feature, many phones and associated switches do not have a mechanism to allow the user to manage multiple calls simultaneously on the same line.

Cisco CallManager Administration effectively enhances the Call Waiting feature to provide this capability for users of Cisco IP Phones (model 794X and 796X series). These Cisco IP Phones include a user interface that gives the user adequate control of multiple, simultaneous calls when interfacing with the Cisco CallManager system. This enhanced functionality allows the Call Waiting feature to be applied to all precedence calls that are directed to these types of phones, even though the user may already be managing other calls. When the user receives a precedence call, the user at a destination phone can decide what to do with any existing calls instead of merely releasing the lower precedence call. For users of these devices, the Cisco CallManager administrator can configure devices as not MLPP Preemption Enabled to take advantage of this function in Cisco CallManager.

Common Network Facility Preemption

Common network facility preemption applies to network resources, such as trunks, in the MLPP system. When a common network facility gets preempted, all existing parties receive notification of the preemption, and the existing connection immediately gets disconnected. The new call gets set up by using the preempted facility in the normal manner without any special notification to the new called party. PRI and T1-CAS trunks on targeted MGCP gateway platforms support this type of preemption in Cisco CallManager.

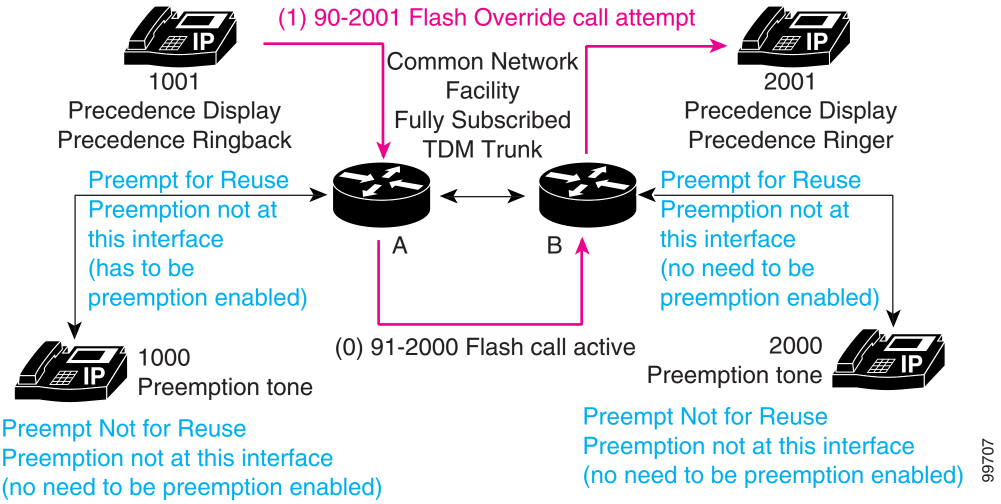
Preemption occurs if a precedence call request is validated and if the requested precedence of the call is greater than the precedence of an existing call through the destination MLPP Preemption Enabled trunk and the trunk is completely busy (that is, cannot handle any more calls). Call processing identifies a call with lower precedence, notifies the connected parties of the preemption for the PRI trunk interface, reserves the channel for subsequent use, and drops the selected lower precedence call. The system uses the reserved channel to establish the connection through the gateway for the precedence call that caused preemption.

For the sequence of steps that takes place during common network facility preemption, see the following examples.

Example 1

Figure 13-7 illustrates an example of common network facility preemption.

Figure 13-7 Common Network Facility Preemption Example



In the example of common network facility preemption, the following sequence of events takes place:

1. User 1000 places a precedence call of precedence level Flash Override to user 2000, who answers the call. In this example, user 1000 dials 90-2000 to place the precedence call. The flash call of precedence level Flash Override specifies active.

   The call uses a common network facility where the two gateways define a fully subscribed TDM trunk.

2. User 1001 next places a higher precedence (executive override) call to user 2001 by dialing 9*-2001. (Assume that the flash call represents the lowest precedence call over gateway A, and users 1000 and 1001 reside in the same MLPP domain.)

   Preemption occurs at gateway A, which is preempted for reuse. Because preemption occurs at this interface, you must ensure that this device is preemption enabled. Gateway B also gets preempted for reuse, but the preemption does not occur at this interface, so this device does not need to be preemption enabled.

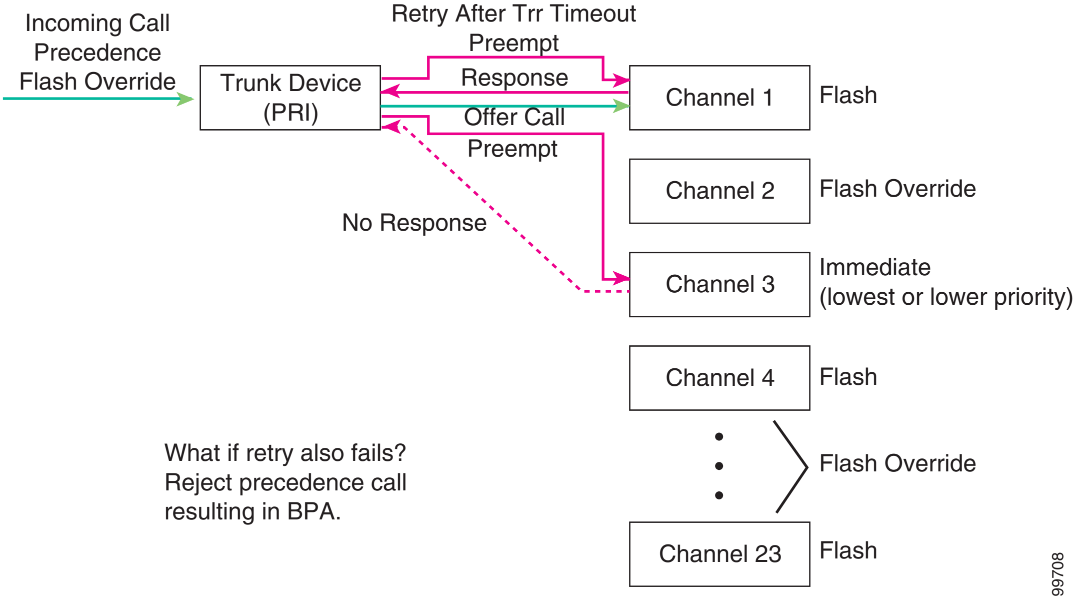
   Users 1000 and 2000 both receive preemption tones. Because both devices are not preempted for reuse and preemption does not occur at these interfaces, you do not need to ensure that these devices are preemption enabled for the preemption to occur.

In this example, almost all events occur instantly. Parties do not need to hang up for common network facility preemption to occur.

Example 2

Figure 13-8 illustrates an example of common network facility preemption with the retry timer Trr. The retry timer Trr provides a mechanism, so if preemption is not successful on one channel, preemption gets retried on another channel. This timer applies only to TDM trunks.

Figure 13-8 Common Network Facility Preemption Example with Retry Timer Trr



In the example of common network facility preemption with the retry timer Trr, the following sequence of events takes place:

1. An incoming call with Flash Override precedence arrives at a PRI trunk device.

   The incoming call causes preemption of channel 3, but a response does not occur within the time that the retry timer Trr specifies.

2. Retry timer Trr expires.

   Channel 3 gets preempted.

3. This preemption causes a response, and the precedence call gets offered on channel 1.

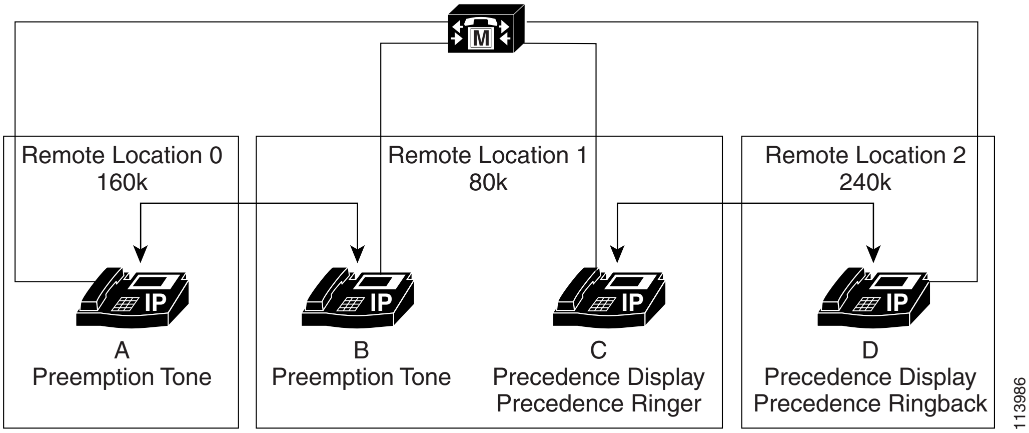
Location-Based Preemption

The following examples illustrate location-based preemption.

Example 1

In the example that follows, the new call and the location-preempted call take place in different devices. See Figure 13-9 for an example of this type of location-based preemption.

Figure 13-9 Location-Based Preemption in Different Devices



This example illustrates the location-based preemption scenario. In the example, three locations exist:

- Remote location 0 (RL0) with phone A and 160K of available bandwidth
- Remote location 1 (RL1) with phones B and C and 80K of available bandwidth
- Remote location 2 (RL2) with phone D and 240K of available bandwidth

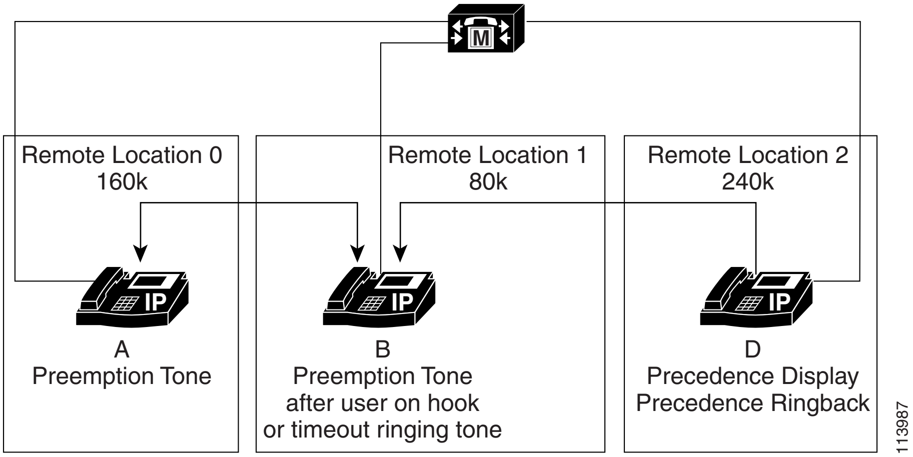
The following sequence of events takes place:

1. A places a call to B with Priority precedence level, and the call becomes active. The available bandwidth specifies 80K in RL0, 0K in RL1, and 240K in RL2.
2. D calls C with Immediate precedence level. D's call preempts the call between A and B because RL1 is out of bandwidth and D's call has higher precedence.
3. The call between D and C completes. The available bandwidth specifies 160K in RL0, 0K in RL1, and 160K in RL2.

Example 2

In the example that follows, the new call and the location preempted call take place in the same device. See Figure 13-10 for an example of this type of location-based preemption.

Figure 13-10 Location-Based Preemption in the Same Device



This example illustrates the location-based preemption scenario. In the example, three locations exist:

- Remote location 0 (RL0) with phone A and 160K of available bandwidth
- Remote location 1 (RL1) with phone B and 80K of available bandwidth
- Remote location 2 (RL2) with phone D and 240K of available bandwidth

The following sequence of events takes place:

1. A places a call to B with Priority precedence level, and the call becomes active. The available bandwidth specifies 80K in RL0, 0K in RL1, and 240K in RL2.
2. D calls B with Immediate precedence level. D’s call preempts the call between A and B because RL1 is out of bandwidth and D’s call has higher precedence.
3. B receives the preemption tone first, and the End call softkey displays.
4. B presses the End softkey, hangs up, or waits for timeout. The call from D to B gets offered to B. When the call from D to B completes, the available bandwidth specifies 160K in RL0, 0K in RL1, and 160K in RL2.

MLPP Announcements

Users who unsuccessfully attempt to place MLPP precedence calls receive various announcements that detail the reasons why a precedence call was blocked.

The following sections discuss specific MLPP announcements:

- Unauthorized Precedence Announcement, page 13-17
- Blocked Precedence Announcement, page 13-18
- Busy Station Not Equipped for Preemption, page 13-18
- Announcements Over Intercluster Trunks, page 13-18

The Supported Tones and Announcements topic in the Annunciator section of the *Cisco CallManager System Guide* discusses MLPP announcements. Refer to the Route Pattern Configuration and Translation Pattern Configuration sections in the *Cisco CallManager Administration Guide* for details of configuring the Precedence Level Exceeded condition that generates the Unauthorized Precedence Announcement.

Additional Information

See the "Related Topics" section on page 13-30.

Unauthorized Precedence Announcement

Users receive an unauthorized precedence announcement when they attempt to make a call with a higher level of precedence than the highest precedence level that is authorized for their line. A user receives an unauthorized precedence announcement when the user dials a precedence call by using a calling pattern for which the user does not have authorization.

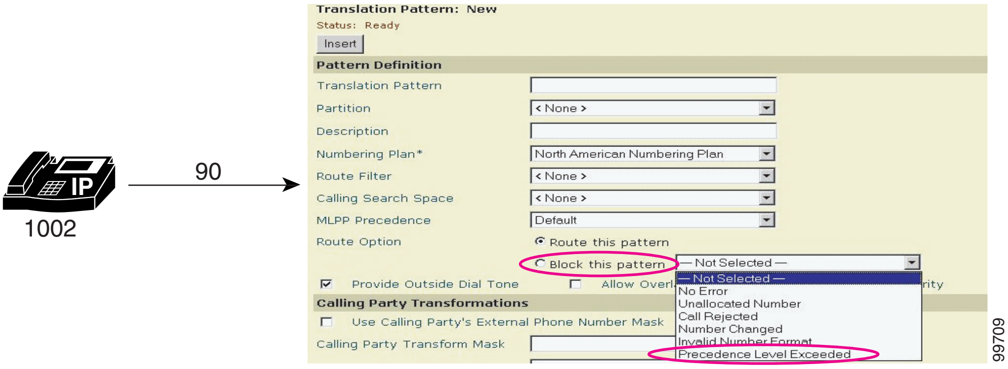
Cisco CallManager recognizes the Precedence Level Exceeded condition only if specific patterns or partitions are configured to block a call attempt that matches the pattern and that indicates the reason that the call is blocked.

To assign authorized calling patterns, access the Route Pattern/Hunt Pilot Configuration and the Translation Pattern Configuration windows in Cisco CallManager Administration. To configure the MLPP Precedence Level Exceeded condition, use the Route Option field of the Route Pattern/Hunt Pilot Configuration and Translation Pattern Configuration windows and choose the Block this pattern option in Cisco CallManager Administration. In the drop-down list box, choose *Precedence Level Exceeded*. Refer to the Route Pattern Configuration and Translation Pattern Configuration sections of the *Cisco CallManager Administration Guide* for details.

Example

Figure 13-11 illustrates an example of a user that receives an unauthorized precedence announcement.

Figure 13-11 Unauthorized Precedence Announcement Example



Translation Pattern: New
Status: Ready
Insert

Pattern Definition
Translation Pattern
Partition < None >
Description
Numbering Plan* North American Numbering Plan
Route Filter < None >
Calling Search Space < None >
MLPP Precedence Default
Route Option ● Route this pattern
○ Block this pattern — Not Selected —
☑ Provide Outside Dial Tone □ Allow Overl… …rity

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

In the example, user 1002 dials 90 to start a precedence call. Nine (9) represents the precedence access digit, and zero (0) specifies the precedence level that the user attempts to use. Because this user is not authorized to make flash override precedence calls (calls of precedence level 0), the user receives an unauthorized precedence announcement.

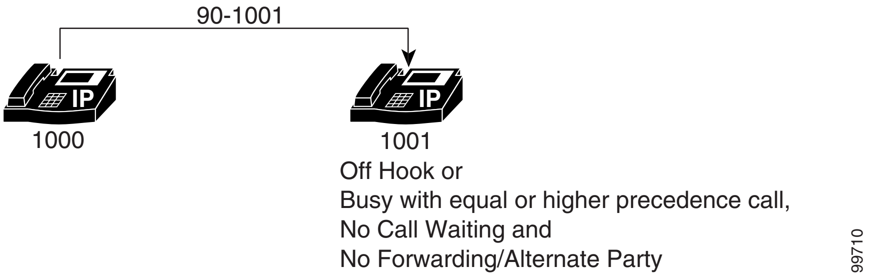
Blocked Precedence Announcement

Users receive a blocked precedence announcement if the destination party for the precedence call is off hook, or if the destination party is busy with a precedence call of an equal or higher precedence and the destination party does not have the Call Waiting nor Call Forward features nor a designated party for alternate party diversion (APD), or due to a lack of a common network resource.

Example

Figure 13-12 provides an example of a blocked precedence announcement.

Figure 13-12 Blocked Precedence Announcement Example


90-1001
IP
IP
1000
1001
Off Hook or
Busy with equal or higher precedence call,
No Call Waiting and
No Forwarding/Alternate Party
99710

In this example, user 1000 makes a precedence call to user 1001 by dialing 90-1001. Because user 1001 is either off hook or busy with a precedence call of - equal or higher precedence level and user 1001 does not have Call Waiting nor Call Forward nor an alternate party that is designed for alternate party diversion, user 1000 receives a blocked precedence announcement.

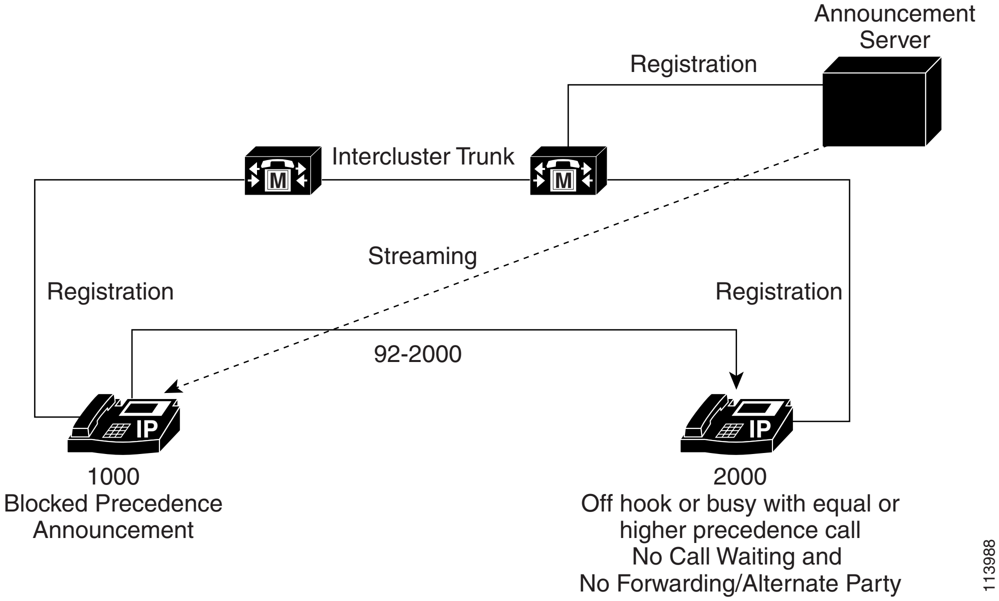
Busy Station Not Equipped for Preemption

Users receive this announcement if the dialed number is nonpreemptable. That is, the dialed number registers as busy and has no call waiting, no call forwarding, and no alternate party designations.

Announcements Over Intercluster Trunks

Figure 13-13 illustrates an instance of an MLPP announcement that is streamed over an intercluster trunk.

Figure 13-13 MLPP Announcement Over an Intercluster Trunk Example



In the example, phones 1000 and 2000 reside on two clusters that an intercluster trunk connects. User 2000 does not have features such as calling waiting and call forwarding configured.

The following sequence of events takes place:

1. User 2000 goes off hook and starts to dial. (Status for User 2000 specifies originating busy and not preemptable.)
2. User 1000 then dials a precedence call over the intercluster trunk to user 2000. Because user 2000 is busy and is not preemptable, the call gets rejected.
3. Because user 1000 originated a precedence call, the call receives precedence treatment, and the announcement server on the remote cluster streams the appropriate Blocked Precedence Announcement (BPA) to 1000 with the switch name and the location of the cluster.

MLPP Numbering Plan Access Control for Precedence Patterns

MLPP uses the calling search spaces and partitions that are defined for users to authenticate and validate MLPP calls and provide access control for precedence patterns.

The maximum precedence of a user gets set at user configuration time. All MLPP-capable station devices get configured as either MLPP-enabled or MLPP-disabled. A device to which a user profile is applied inherits the precedence level of that user with respect to precedence calls that are initiated from that device. A device that has a default user assigned inherits a Routine precedence level for the default user.

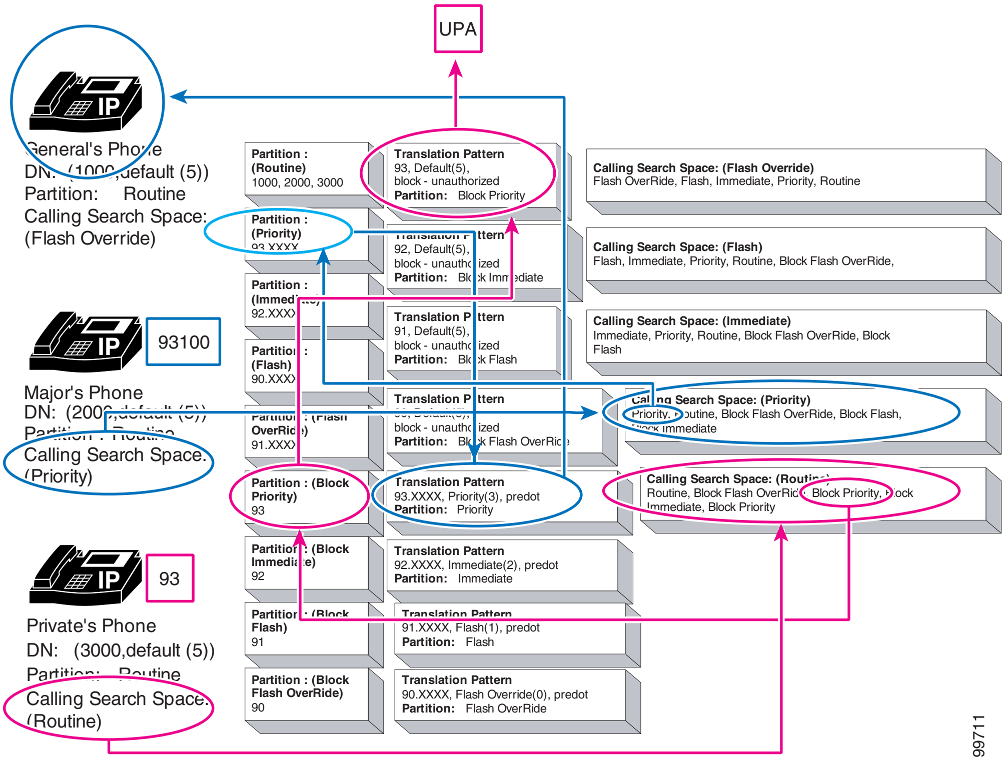
Configuration of the calling search space(s) (CSS) that is associated with the calling party controls a user's ability to dial a precedence pattern (that is, to initiate a precedence call). Cisco CallManager does not provide for explicit configuration of an explicit maximum allowed precedence value.

The following example illustrates the differences in access to precedence calls for two users who try to place a priority-level precedence call to a third user.

Example

Figure 13-14 provides an example of MLPP numbering plan access control for precedence patterns.

Figure 13-14 MLPP Numbering Plan Access Control for Precedence Patterns Example


UPA
IP
General's Phone
DN: (1000,default (5))
Partition: Routine
Calling Search Space: (Flash Override)
IP
93100
Major's Phone
DN: (2000,default (5))
Partition : Routine
Calling Search Space: (Priority)
IP
93
Private's Phone
DN: (3000,default (5))
Partition: Routine
Calling Search Space: (Routine)
Partition : (Routine) 1000, 2000, 3000
Partition : (Priority) 93.XXXX
Partition : (Immediate) 92.XXXX
Partition : (Flash) 90.XXXX
Partition : (Flash OverRide) 91.XXXX
Partition : (Block Priority) 93
Partition : (Block Immediate) 92
Partition : (Block Flash) 91
Partition : (Block Flash OverRide) 90
Translation Pattern 93, Default(5), block - unauthorized Partition: Block Priority
Translation Pattern 92, Default(5), block - unauthorized Partition: Block Immediate
Translation Pattern 91, Default(5), block - unauthorized Partition: Block Flash
Translation Pattern 90, Default(5), block - unauthorized Partition: Block Flash OverRide
Translation Pattern 93.XXXX, Priority(3), predot Partition: Priority
Translation Pattern 92.XXXX, Immediate(2), predot Partition: Immediate
Translation Pattern 91.XXXX, Flash(1), predot Partition: Flash
Translation Pattern 90.XXXX, Flash Override(0), predot Partition: Flash OverRide
Calling Search Space: (Flash Override) Flash OverRide, Flash, Immediate, Priority, Routine
Calling Search Space: (Flash) Flash, Immediate, Priority, Routine, Block Flash OverRide,
Calling Search Space: (Immediate) Immediate, Priority, Routine, Block Flash OverRide, Block Flash
Calling Search Space: (Priority) Priority, Routine, Block Flash OverRide, Block Flash, Block Immediate
Calling Search Space: (Routine) Routine, Block Flash OverRide, Block Priority, Block Immediate, Block Priority
99711

The table defines three users in this illustration:

User	Directory Number (DN)	Partition	Calling Search Space (CSS)
General	1000	Routine	Flash Override
Major	2000	Routine	Priority
Private	3000	Routine	Routine

The example shows the use of partitions and calling search spaces to limit access to precedence calls.

If private 3000 tries to place a precedence call by dialing the precedence pattern 93, the following events take place:

- Call processing searches for private 3000's calling search space, which is the Routine CSS.
- Within private 3000's Routine CSS, call processing finds the Block Priority partition.
- In the Block Priority partition, call processing finds the pattern 93 and goes to translation pattern 93.
- Translation pattern 93 determines that priority calls are blocked for this user (DN), and call processing issues an unauthorized precedence announcement (UPA).

If major 2000 places a precedence call by dialing the digits 931000, the following events take place:

- Call processing searches for major 2000's calling search space, which is the Priority CSS.
- Within major 2000's Priority CSS, call processing finds the Priority partition.

- In the Priority partition, call processing finds the pattern 93.XXXX and goes to translation pattern 93.XXXX.
- Translation pattern 93.XXXX determines that priority calls are authorized for this user (DN). Call processing therefore completes the Priority-level precedence call to user 1000, the general.

MLPP Trunk Selection

MLPP trunk selection entails hunting for available trunks by using route lists and route groups. In Cisco CallManager Administration, you can configure a route list and associated route group(s) to route calls to several gateways via a single dial pattern to find an available channel. Although a route list has many trunk resources to which the route list can route calls, the individual resources may spread across many gateways.

When no available trunk resource is identified in a collection of gateways (that is, a route list and route group configuration), Cisco CallManager attempts to initiate preemption of a lower level precedence shared resource in the collection. Two methods exist for subsequently searching for a preemptable channel within a route list and route group configuration.

Method 1

Configure a route list and a separate route group for each available route (trunk interface). Designate one route group as the Direct route group and designate the other route groups as Alternate route groups. Add the Direct Route trunk interface (gateway) as the only member of the Direct route group. Add the Alternate Route gateways to the individual Alternate route groups. Associate the route groups with the route list, configuring the Direct route group as the first route group in the route list, and choose the Top Down distribution algorithm for each route group association.

Using this configuration, the Direct gateway in the Direct route group gets searched for an idle channel first. If no idle channel is found in the Direct gateway, the system initiates preemptive trunk selection for this Direct gateway as follows:

- Call processing chooses the Direct route and offers the call to this gateway device to determine whether the gateway device can initiate preemption.
- If the Direct gateway device rejects the precedence call request (that is, the gateway device cannot initiate preemption), choose the next route group in the route list as the current route. Continue this sequence until an idle channel is found on the current gateway, or until the current gateway device has initiated preemption, or until all gateway devices in the route list and route group collection are searched.

Method 2

Configure a route list and a single route group. Add trunk interfaces (gateways) to the route group and position the Direct Route gateway as the first gateway in the route group. Associate the route group with the route list and choose the Top Down distribution algorithm. With this configuration, the system searches all gateways in the route group for an idle channel first. If no idle channel is found in any gateway in the route group, preemptive trunk selection begins with the first gateway in the route group (that is, the Direct Route gateway) as follows:

- Call processing chooses a current route from the collection on the basis of the distribution algorithm and offers the call to this gateway device to determine whether the gateway device can initiate preemption.

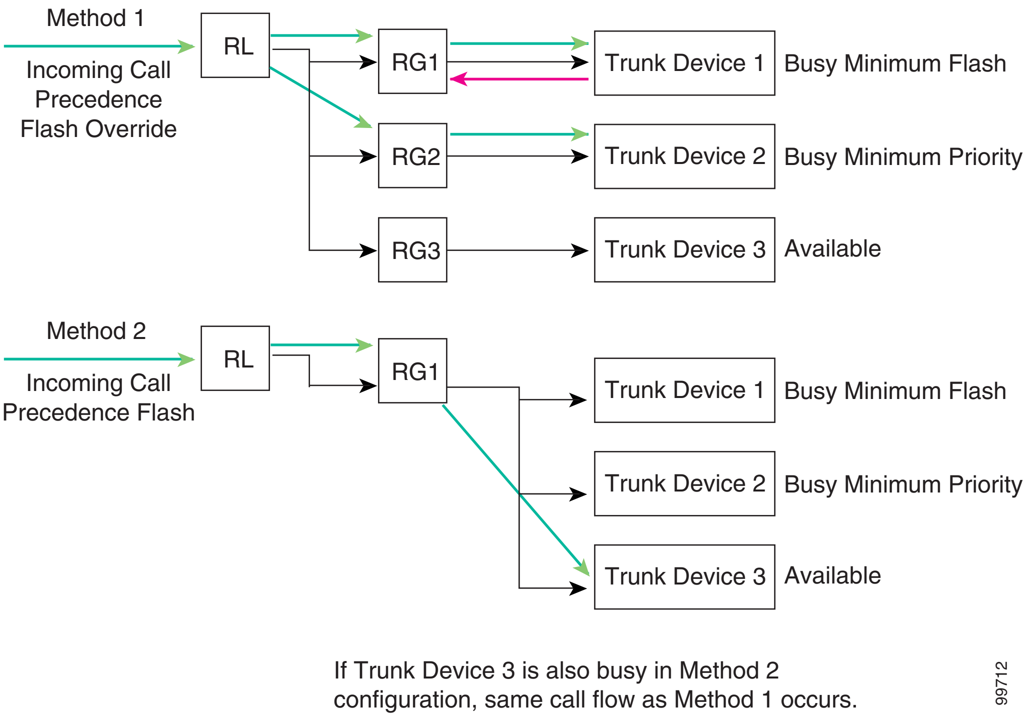
- If the current gateway device rejects the precedence call request (that is, the gateway device cannot initiate preemption), call processing chooses the next gateway in the collection as the current route and continues this sequence until a gateway device initiates preemption or until all gateway devices in the route list and route group collection have been searched.

Example

The following example illustrates two methods for finding an available trunk device when an incoming flash-level precedence call seeks an available trunk device.

Figure 13-15 provides an example of MLPP trunk selection using route lists and route groups to hunt for an available trunk device.

Figure 13-15 MLPP Trunk Selection (Hunting) Example



In method 1, the following sequence of events takes place:

1. An incoming flash-level precedence call reaches route list RL and first goes to route group RG1, which directs the call to Trunk Device1, which is busy.

   For Trunk Device1, calls must be of a higher precedence than flash to preempt calls that are using this device.

2. The call therefore seeks the next route group in route list RL, which is route group RG2. Route group RG2 contains Trunk Device2, which is also busy, but precedence calls of a precedence level higher than Priority can preempt Trunk Device2.

   Because this call is a higher precedence call, the call preempts the existing call on Trunk Device2.

In method 2, the following sequence of events takes place:

1. An incoming flash-level precedence call reaches route list RL, which contains only one route group, RG1.

2. Route group RG1 contains three trunk devices.

   Of the three trunk devices in RG1, Trunk Device1 and Trunk Device2 register as busy, so the system offers the call to Trunk Device3, which is available.

MLPP Hierarchical Configuration

MLPP settings for devices follow this hierarchy:

- If a device MLPP Indication is set to *Off*, the device cannot send indication of MLPP calls. If the device MLPP Preemption is set to *Disabled*, the device cannot preempt calls. These settings override the device's device pool settings.
- If a device MLPP Indication is set to *On*, the device can send indication of MLPP calls. If the device's MLPP Preemption is set to *Forceful*, the device can preempt calls. These settings override the device's device pool settings.
- If a device's MLPP Indication is set to *Default*, the device inherits its ability to send indication of MLPP calls from the device's device pool. If the device MLPP Preemption is set to *Default*, the device inherits its ability to preempt calls from the device's device pool.

MLPP settings for device pools follow this hierarchy:

- If a device pool MLPP Indication is set to *Off*, devices in the device pool cannot send indication of MLPP calls. If the device pool MLPP Preemption is set to *Disabled*, devices in the device pool cannot preempt calls. These settings override the MLPP enterprise parameter settings.
- If a device pool MLPP Indication is set to *On*, devices in the device pool can send indication of MLPP calls. If the device pool MLPP Preemption is set to *Forceful*, devices in the device pool can preempt calls. These settings override the MLPP enterprise parameter settings.
- If a device pool MLPP Indication is set to *Default*, the device inherits its ability to send indication of MLPP calls from the MLPP Indication Status enterprise parameter. If the device pool MLPP Preemption is set to *Default*, the device pool inherits its ability to preempt calls from the MLPP Preemption Setting enterprise parameter.

The MLPP Indication Status enterprise parameter defines the indication status of device pools and device pools in the enterprise, but nondefault settings for device pools and individual devices can override its value. The default value for this enterprise parameter specifies *MLPP Indication turned off*.

The MLPP Preemption Setting enterprise parameter defines the preemption ability for device pools and devices in the enterprise, but nondefault settings for device pools and individual devices can override its value. The default value for this enterprise parameter specifies *No preemption allowed*.

The MLPP Domain Identifier enterprise parameter specifies the MLPP domain. The MLPP service applies only to a domain; that is, only to the subscribers and the network and access resources that belong to a particular domain. Connections and resources that belong to a call from an MLPP subscriber get marked with a precedence level and an MLPP domain identifier. Only calls of higher precedence from MLPP users in the same domain can preempt lower precedence calls in the same domain.

Service Parameter Special Trace Configuration

MLPP issues a service parameter for tracing.

Refer to the *Cisco CallManager Serviceability System Guide* and the *Cisco CallManager Serviceability Administration Guide* for details.

CDR Recording for Precedence Calls

MLPP precedence calls generate call detail records (CDRs). The CDR identifies the precedence level of the precedence call.

The same precedence levels of the call legs generally apply. With transfer or conference calls, the precedence levels can differ; therefore, Cisco CallManager CDRs identify the precedence level of each leg of the call.

Cisco CallManager CDRs document the preemption value for preempted call terminations.

Refer to the *Cisco CallManager Serviceability System Guide* and the *Cisco CallManager Serviceability Administration Guide* for details.

Line Feature Interaction

MLPP interacts with line features as described in the following sections:

- Call Forward, page 13-24
- Call Transfer, page 13-25
- Shared Lines, page 13-25
- Call Waiting, page 13-25

Call Forward

MLPP interacts with the call forward features as described in the following list:

- Call Forward Busy
  - You optionally can configure a preconfigured Precedence Alternate Party target for any MLPP-enabled station.
  - Cisco CallManager applies the Call Forward Busy feature to forward a precedence call in the usual manner prior to applying any Precedence Alternate Party Diversion procedures to the call.
  - If the incoming precedence call is of equal or lower precedence than the existing call, call processing invokes normal call-forwarding behavior.
  - If the destination station for a precedence call is nonpreemptable (that is, not MLPP-configured), call processing invokes call-forwarding behavior.
  - The system preserves precedence of calls across multiple forwarded calls.
  - If the incoming precedence call is of higher precedence than the existing call, preemption occurs. Both the preempted parties in the active call receive a continuous preemption tone until the station to which the precedence call is directed hangs up. After hanging up, the station to which the precedence call is directed receives precedence ringing. The destination station connects to the preempting call when the station goes off hook.
- Call Forward No Answer
  - For calls of Priority precedence level and above, call processing preserves the precedence level of calls during the forwarding process and may preempt the forwarded-to user.
  - If an Alternate Party is configured for the destination of a precedence call, call processing diverts the precedence call to the Alternate Party after the Precedence Call Alternate Party timeout expires.

If no Alternate Party setting is configured for the destination of a precedence call, call processing diverts the precedence call to the Call Forward No Answer setting.

- Normally, precedence calls route to users and not to the voice-messaging system. The administrator sets the Use Standard VM Handling For Precedence Calls enterprise parameter to avoid routing precedence calls to voice-messaging systems. Refer to the "Setting the Enterprise Parameters for MLPP" section on page 13-29 for details.

Call Transfer

MLPP interacts with the call-transfer feature. For blind transfers and consult transfers, each connection of the transferred call, including the consult call, maintains the precedence that the connection was assigned when the call was established.

Shared Lines

MLPP interacts with shared lines. A shared-line appearance with a call on hold may be preempted to establish a higher precedence call to another terminal with the same directory number (DN). In this case, the original held call does not disconnect, and the precedence call connects. After the precedence call ends, the user may retrieve the original held call.

Call Waiting

MLPP interacts with the call-waiting feature as described in the following list:

- When conflicts arise between call-waiting status and MLPP precedence calls due to the lack of network resources, the call gets preempted.
- When a precedence call is offered to a destination station that is configured with call waiting, the following behaviors take place:
  - If the requested precedence is higher than the existing call precedence, the existing call gets preempted. If the destination user is nonpreemptable, call processing invokes normal call-waiting behavior and alerting. If the precedence call is of Priority precedence level or higher, the destination user receives precedence call-waiting tones and cadences.
  - If the requested precedence level is the same as the existing call precedence, call processing invokes normal call-waiting behavior. If the precedence call is of Routine precedence, call processing alerts the destination with standard call-waiting tones. If the precedence call is of Priority or higher precedence, call processing alerts the destination with precedence call-waiting tones.
  - If the requested precedence level is lower than the existing call precedence, call processing invokes normal call-waiting behavior. If the precedence call is of Routine precedence, call processing alerts the destination with standard call-waiting tones. If the precedence call is of Priority or higher precedence, call processing alerts the destination with precedence call-waiting tones.
  - When a device has more than one appearance, the destination user may place a lower precedence call on hold to acknowledge receipt of a higher precedence call. After the higher precedence call ends, the destination user may resume the held, lower precedence call.

Call Preservation

Any MGCP trunk call or connection that is preserved according to the Cisco CallManager Call Preservation feature preserves its precedence level and MLPP domain after invoking the Call Preservation feature. After the device registers with Cisco CallManager, the system only preserves the preserved calls at the device layer in the Cisco CallManager system. As a result, the preserved calls gets treated as two disjointed half calls. If preemption does occur on these devices, only one leg can follow preemption protocol to the other leg. The system detects call termination only through closure of the RTP port.

Automated Alternate Routing

The Automated Alternate Routing (AAR) for Insufficient Bandwidth feature, an extension of AAR, provides a mechanism to automatically fall back to reroute a call through the Public Switched Telephone Network (PSTN) or other network by using an alternate number when the Cisco CallManager blocks the call due to insufficient location bandwidth. With this feature, the caller does not need to hang up and redial the called party.

If a precedence call attempt meets a condition that invokes the AAR service, the precedence call gets rerouted through the PSTN or other network as specified by the AAR configuration. Cisco CallManager handles the precedence nature of the call in the same manner as if the call originally had been routed through the PSTN or other network, based on the MLPP Indication Enabled and MLPP Preemption Enabled nature of the network interface through which the call is routed.

For details of configuring Automated Alternate Routing, refer to the Automated Alternate Routing Group Configuration section of the *Cisco CallManager Administration Guide*.

MGCP and PRI Protocol

MLPP supports Common Network Facility Preemption only for T1-CAS and T1-PRI (North American) interfaces on targeted Voice over IP gateways that Cisco CallManager controls by using MGCP protocol and that have been configured as MLPP Preemption Enabled.

Secure Endpoints and Secure Communications

The traditional Department of Defense (DOD) TDM network uses legacy analog secure telephone units (STUs) and BRI secure telephone equipment (STEs) as secure endpoints, which are critical for secure communication. The newly developed IP STE also requires support to reduce the need for legacy equipment. Cisco CallManager supports the Skinny Client Control Protocol for these devices. Modem relay provides secure communication and uses the V.150 protocol.

Interactions and Restrictions

The following sections describe the interactions and restrictions for MLPP.

- Interactions, page 13-27
- Restrictions, page 13-27

Interactions

MLPP interacts with the following Cisco CallManager features as follows:

- Extension Mobility—The MLPP service domain remains associated with a user device profile when a user logs in to a device by using extension mobility. The MLPP Indication and Preemption settings also propagate with extension mobility. If either the device or the device profile do not support MLPP, these settings do not propagate.
- Immediate Divert—Immediate Divert diverts calls to voice-messaging mail boxes regardless of the type of call (for example, a precedence call). When Alternate Party Diversion (call precedence) is activated, Call Forward No Answer (CFNA) also gets deactivated.
- IP Manager Assistant (IPMA)—MLPP interacts with IPMA as follows:
  - When IPMA handles an MLPP precedence call, IPMA preserves call precedence.
  - IPMA filters MLPP precedence calls in the same manner as it filters all other calls. The precedence of a call does not affect whether the call is filtered.
  - Because IPMA does not register the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.
- Resource Reservation Protocol (RSVP)—RSVP supports MLPP inherently. The "RSVP-Based MLPP" section in the Resource Reservation Protocol chapter of the *Cisco CallManager System Guide* explains how MLPP functions when RSVP is activated.

Restrictions

The following restrictions apply to MLPP:

- Common Network Facility Preemption support exists only for T1-CAS and T1-PRI (North American) interfaces on targeted Voice over IP gateways that Cisco CallManager controls by using MGCP protocol and that have been configured as MLPP Preemption Enabled.
- User Access Channel support exists only for the following Cisco IP Phone models, which must be configured as MLPP Preemption Enabled:
  - Cisco 796X series IP Phone
  - Cisco 794X series IP Phone
- IOS gateways support SCCP interface to CCM. Hence, they support BRI and analog phones which appear on Cisco Call Manger as supported phone models.
- Only MLPP Indication Enabled devices generate MLPP-related notifications, such as tones and ringers. If a precedence call terminates at a device that is not MLPP Indication Enabled, no precedence ringer gets applied. If a precedence call originates from a device that is not MLPP Indication Enabled, no precedence ringback tone gets applied. If a device that is not MLPP Indication Enabled is involved in a call that is preempted (that is, the other side of the call initiated preemption), no preemption tone gets applied to the device.
- For phones, devices that are MLPP indication disabled (that is, MLPP Indication is set to *Off*) cannot be preempted.

  For trunks, MLPP indication and preemption function independently.
- Cisco CallManager does not support the Look Ahead for Busy (LFB) option.
- Intercluster trunk MLPP carries precedence information through dialed digits. Domain information does not get preserved and must be configured per trunk for incoming calls.

- 729 Annex A is supported.
- Various location bandwidth preemption limitations exist.
- For the DRSN, CDRs represent precedence levels with values 0, 1, 2, 3, and 4 where 0 specifies Executive Override and 4 specifies Routine, as used in DSN. CDRs thus do not use the DRSN format.
- Location preemption does not apply to video calls. In Cisco CallManager, audio bandwidth and video bandwidth get tracked separately. Video calls do not get preempted.
- MLPP-enabled devices are not supported in line groups. As such, Cisco recommends the following guidelines:
  - MLPP-enabled devices should not be configured in a line group. Route groups, however, are supported. Both trunk selection and hunting methods are supported.
  - If an MLPP-enabled device is configured in a line group or route group, in the event of preemption, if the route list does not lock onto the device, the preempted call maybe rerouted to other devices in the route/hunt list and preemption indication maybe returned only after no devices are able to receive the call.
  - Route lists can be configured to support either of two algorithms of trunk selection and hunting for precedence calls. In method 1, perform a preemptive search directly. In method 2, first perform a friendly search. If this search is not successful, perform a preemptive search. Method 2 requires two iterations through devices in a route list.

    If route lists are configured for method 2, in certain scenarios involving line groups, route lists may seem to iterate through the devices twice for precedence calls.
- Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.

Refer to the "MLPP Configuration Checklist" section on page 13-28 for configuration details.

Installing and Activating MLPP

MLPP, a system feature, comes standard with Cisco CallManager software and does not require special installation.

MLPP Configuration Checklist

Table 13-1 provides a checklist to configure MLPP.

Table 13-1 MLPP Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure a device pool for which associated devices can make MLPP calls.	Device Pool Configuration, *Cisco CallManager Administration Guide*
Step 2	Set enterprise parameters to enable MLPP indication and preemption. If individual devices and devices in device pools have MLPP settings of *Default*, the MLLP-related enterprise parameters apply to these devices and device pools.	Setting the Enterprise Parameters for MLPP, page 13-29 Enterprise Parameters Configuration, *Cisco CallManager Administration Guide*

Table 13-1 MLPP Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 3	Configure partitions and Calling Search Spaces (CSS) that allow users (calling parties and their associated devices) to place precedence calls that use MLPP.	Partition Configuration, *Cisco CallManager Administration Guide* Calling Search Space Configuration, *Cisco CallManager Administration Guide*
Step 4	Configure route patterns/hunt pilots that specify MLPP precedence level and route options for MLPP calls.	Route Pattern Configuration, *Cisco CallManager Administration Guide*
Step 5	Configure translation patterns that specify MLPP precedence level and route options for MLPP calls.	Translation Pattern Configuration, *Cisco CallManager Administration Guide*
Step 6	Configure gateways that specify an MLPP domain for MLPP calls. The following gateway types apply: • Cisco Catalyst 6000 24 port FXS Gateway • Cisco Catalyst 6000 E1 VoIP Gateway • Cisco Catalyst 6000 T1 VoIP Gateway • Cisco DE-30+ Gateway • Cisco DT-24+ Gateway • H.323 Gateway **Note** Some gateway types allow configuration of MLPP Indication and MLPP Preemption settings.	Gateway Configuration, *Cisco CallManager Administration Guide*
Step 7	Configure Cisco IP Phones that specify an MLPP domain for MLPP calls. **Note** Some phone types allow configuration of MLPP Indication and MLPP Preemption settings.	Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
Step 8	Configure the directory number that will place an MLPP call.	Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
Step 9	Configure the User Device Profile of the user that will make an MLPP call.	Device Profile Configuration, *Cisco CallManager Administration Guide*
Step 10	Configure the Device Profile Default for devices that will make MLPP calls.	Default Device Profile Configuration, *Cisco CallManager Administration Guide*
Step 11	Notify users that the MLPP service is available.	Refer to the phone documentation for instructions on how users access MLPP features on their Cisco IP Phone.

Setting the Enterprise Parameters for MLPP

Cisco CallManager provides the following enterprise parameters that apply to MLPP. Set the MLPP-related enterprise parameters as indicated to allow MLPP service.

- MLPP Domain Identifier—Default specifies zero (0). Set this parameter to define a domain. Because MLPP service applies to a domain, Cisco CallManager only marks connections and resources that belong to calls from MLPP users in a given domain with a precedence level. Cisco CallManager can preempt only lower precedence calls from MLPP users in the same domain.

  Note You must reset all devices for a change to this parameter to take effect.

- MLPP Indication Status—Default specifies *MLPP Indication turned off*. This parameter specifies whether devices use MLPP tones and special displays to indicate MLPP precedence calls. To enable MLPP indication across the enterprise, set this parameter to *MLPP Indication turned on*.

  Note You must reset all devices for a change to this parameter to take effect.

- MLPP Preemption Setting—Default specifies *No preemption allowed*. This parameter determines whether devices should apply preemption and preemption signaling (such as preemption tones) to accommodate higher precedence calls. To enable MLPP preemption across the enterprise, set this parameter to *Forceful Preemption*.

  Note You must reset all devices for a change to this parameter to take effect.

- Precedence Alternate Party Timeout—Default specifies 30 seconds. In a precedence call, if the called party subscribes to alternate party diversion, this timer indicates the seconds after which Cisco CallManager will divert the call to the alternate party if the called party does not acknowledge preemption or does not answer a precedence call.
- Use Standard VM Handling For Precedence Calls—Default specifies *False*. This parameter determines whether a precedence call will forward to the voice-messaging system. If the parameter is set to False, precedence calls do not forward to the voice-messaging system. If the parameter is set to True, precedence calls forward to the voice-messaging system. For MLPP, the recommended setting for this parameter is False, as users, not the voice- -messaging system, should always answer precedence calls.

For more information about enterprise parameters, refer to the Enterprise Parameters Configuration chapter of the *Cisco CallManager Administration Guide*.

Additional Information

See the "Related Topics" section on page 13-30.

Related Topics

- Call Admission Control, *Cisco CallManager System Guide*
- Resource Reservation Protocol, *Cisco CallManager System Guide*
- Device Pool Configuration, *Cisco CallManager Administration Guide*
- MLPP Domain Configuration, *Cisco CallManager Administration Guide*
- Enterprise Parameters Configuration, *Cisco CallManager Administration Guide*
- Automated Alternate Routing Group Configuration, *Cisco CallManager Administration Guide*

- Partition Configuration, *Cisco CallManager Administration Guide*
- Calling Search Space Configuration, *Cisco CallManager Administration Guide*
- Route Pattern Configuration, *Cisco CallManager Administration Guide*
- Translation Pattern Configuration, *Cisco CallManager Administration Guide*
- Annunciator, *Cisco CallManager System Guide*
- Annunciator Configuration, *Cisco CallManager Administration Guide*
- Gateway Configuration, *Cisco CallManager Administration Guide*
- Trunk Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Device Profile Configuration, *Cisco CallManager Administration Guide*
- Default Device Profile Configuration, *Cisco CallManager Administration Guide*
- Annunciator, *Cisco CallManager System Guide*
- Annunciator Configuration, *Cisco CallManager Administration Guide*
- Route Pattern Configuration, *Cisco CallManager Administration Guide*
- Translation Pattern Configuration, *Cisco CallManager Administration Guide*
- Locations, *Cisco CallManager System Guide*
- MLPP Domain Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco IP Phone Administration Guide for Cisco CallManager, Cisco IP Phone Models 7960G and 7940G*

CHAPTER 14

Custom Phone Rings

This chapter describes how you can customize the phone ring types that are available at your site by creating your own PCM files and editing the Ringlist.xml file.

This chapter covers the following topics:

- Introducing Custom Phone Rings, page 14-1
- Customizing and Modifying Configuration Files, page 14-2
- Ringlist.xml File Format Requirements, page 14-2
- PCM File Requirements for Custom Ring Types, page 14-3
- Configuring a Custom Phone Ring, page 14-3

Introducing Custom Phone Rings

Cisco IP Phones ship with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco CallManager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist.xml) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco CallManager server.

You can get a copy of the Ringlist.xml file from the system using the following admin cli “file” commands:

- admin:file
  - file list*
  - file view*
  - file search*
  - file get*
  - file dump*
  - file tail*
  - file delete*

Customizing and Modifying Configuration Files

You can modify configuration files (for example, edit the xml files) and add customized files (for example, custom ring tones, call back tones, phone backgrounds) to the TFTP directory. You can modify files and/or add customized files to the TFTP directory in Cisco IPT Platform Administration, from the TFTP Server File Upload page. Refer to the *Cisco IP Telephony Platform Administration Guide* for information on how to upload files to the TFTP folder on a Cisco CallManager server.

Ringlist.xml File Format Requirements

The Ringlist.xml file defines an XML object that contains a list of phone ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that will display on the Ring Type menu on a Cisco IP Phone for that ring.

The CiscoIPPhoneRinglist XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRinglist>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRinglist>
```

The following characteristics apply to the definition names:

- DisplayName defines the name of the custom ring for the associated PCM file that will display on the Ring Type menu of the Cisco IP Phone.
- FileName specifies the name of the PCM file for the custom ring to associate with DisplayName.

Tip The DisplayName and FileName fields must not exceed 25 characters.

The following example shows a Ringlist.xml file that defines two phone ring types:

```
<CiscoIPPhoneRinglist>
   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.raw</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.raw</FileName>
   </Ring>
</CiscoIPPhoneRinglist>
```

Tip You must include the required DisplayName and FileName for each phone ring type. The Ringlist.xml file can include up to 50 ring types.

PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet the following requirements for proper playback on Cisco IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- mu-law compression
- Maximum ring size—16080 samples
- Minimum ring size—240 samples
- Number of samples in the ring evenly divisible by 240
- Ring starts and ends at the zero crossing.
- To create PCM files for custom phone rings, you can use any standard audio editing packages that support these file format requirements.

Configuring a Custom Phone Ring

The following procedure applies to creating custom phone rings for only the Cisco IP Phone models 7940, 7960, and 7970.

Procedure

Step 1 Create a PCM file for each custom ring (one ring per file). Ensure that the PCM files comply with the format guidelines that are listed in the "PCM File Requirements for Custom Ring Types" section on page 14-3.

Step 2 Use an ASCII editor to edit the Ringlist.xml file. See the "Ringlist.xml File Format Requirements" section on page 14-2 for information on how to format this file, along with a sample Ringlist.xml file.

Step 3 Save your modifications and close the Ringlist.xml file.

Step 4 Upload the Ringlist.xml file by using the web page interface. Refer to the *Cisco IP Telephony Platform Administration Guide*.

Step 5 To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco CallManager Serviceability or disable and reenable the "Enable Caching of Constant and Bin Files at Startup" TFTP service parameter (located in the Advanced Service Parameters).

Additional Information

See the "Related Topics" section on page 14-3.

Related Topics

- Cisco TFTP, *Cisco CallManager System Guide*
- Service Parameters Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- Cisco IP Phone Administration documentation for Model 7940, 7960, and 7970
- *Cisco IP Telephony Platform Administration Guide*

CHAPTER 15

Cisco WebDialer

Cisco WebDialer, used in conjunction with Cisco CallManager, allows Cisco IP Phone users to make calls from web and desktop applications.

This chapter provides the following information about Cisco WebDialer:

- Introducing Cisco WebDialer, page 15-1
- Redundancy, page 15-2
- System Requirements for Cisco WebDialer, page 15-3
- Interactions and Restrictions, page 15-3
- Installing and Activating Cisco WebDialer, page 15-4
- Configuring Cisco WebDialer, page 15-5
- Related Topics, page 15-13

Introducing Cisco WebDialer

Cisco WebDialer, which is installed on a Cisco CallManager server and used in conjunction with Cisco CallManager, allows Cisco IP Phone users to make calls from web and desktop applications. For example, Cisco WebDialer uses hyperlinked telephone numbers in a company directory to allow users to make calls from a web page by clicking on the telephone number of the person that they are trying to call.

Cisco WebDialer includes the following two main components:

- Webdialer Servlet, page 15-1
- Redirector Servlet, page 15-2

Webdialer Servlet

The Webdialer servlet, a Java servlet, allows Cisco CallManager users in a specific cluster to make and complete calls, as well as to access their phone and line configuration.

An application can interact with the Webdialer servlet through two interfaces:

- The SOAP over HTTP interface—This interface that is based on the Simple Object Access Protocol (SOAP) gets used to develop desktop applications such as Microsoft Outlook Add-in and SameTime Client Plug-in. Developers can use the isClusterUserSoap interface to design multicluster applications that require functionality similar to a Redirector servlet.

- HTML over HTTPS interface—This interface that is based on the HTTPS protocol gets used to develop web-based applications. Developers who use this interface can use the Redirector servlet for designing multicluster applications.

Redirector Servlet

The Redirector servlet, a Java-based Tomcat servlet, finds the Cisco CallManager cluster for a request that a Cisco WebDialer user makes. It redirects that request to the specific Cisco WebDialer server that is located in that user's Cisco CallManager cluster. Availability of the Redirector servlet occurs only for multicluster applications and only for applications that are developed by using HTML over HTTPS interfaces.

Example of Cisco WebDialer Using the Redirector Servlet

For example, consider three clusters, each one in a single city such as San Jose (SJ-CM), Dallas (D-CM), and New York (NY-CM). Each cluster contains three Cisco CallManager servers with Webdialer servlets that have been configured for Cisco CallManager servers SJ-CM1, D-CM2, and NY-CM3.

The system administrator configures the Webdialer servlets on any Cisco CallManager server by entering the IP address of that specific Cisco CallManager server in the *List of WebDialers* service parameter (see the "Setting Service Parameters for the Webdialer Servlet" section on page 15-6). For information on configuring Webdialer and Redirector servlets, refer to the "Configuring the Webdialer Servlet" section on page 15-6 and the "Configuring the Redirector Servlet (Optional)" section on page 15-9.

When a user who is located in San Jose clicks on a telephone number in the corporate directory search window that Cisco WebDialer enables, the following actions happen:

1. The Cisco CallManager server sends an initial *makeCall* HTTPS request to the Redirector servlet.
2. If this request is received for the first time, the Redirector servlet reads the Cisco WebDialer server cookie and finds it empty.

   For a repeat request, the Redirector servlet reads the IP address of the Cisco WebDialer server that previously serviced the client and sends a *isClusterUser* HTTPS request only to that server.
3. The Redirector servlet sends back a response that asks for information, which results in the authentication dialog box opening for the user.
4. The user enters the Cisco CallManager user ID and password and clicks the **Submit** button.
5. The Redirector servlet reads only the user identification from this information and sends a *isClusterUser* HTTPS request to each Cisco WebDialer server that the system administrator has configured.
6. The Redirector servlet redirects the original request from the user to SJ-CM1.

Additional Information

See the "Related Topics" section on page 15-13.

Redundancy

Because redundancy is important for applications that are running in a multicluster environment, this section describes one method to achieve that redundancy.

If a single Redirector servlet is supporting multiple WebDialers in a multicluster environment, it provides a single point of failure. For example, in Figure 15-1, a Redirector servlet runs on the San Jose cluster and also services the New York and Dallas clusters. If this Redirector servlet fails to run on the San Jose cluster, the users who are serviced by all three clusters cannot use Cisco WebDialer.

To avoid this single point of failure, configure Redirector servlets for each cluster. If the directory search window points to a URL such as https://sanjoseclustercompany.com:8443/webdialer/Redirector, change that URL to a virtual link such as https://webdialer-service.company.com/webdialer/Redirector. This virtual link points to a virtual machine that is using a Cisco DistributedDirector. All the Redirector servlets operate behind this virtual link.

For more information on installing and configuring Cisco DistributedDirector, refer to the suite of documents for Cisco DistributedDirector.

Additional Information

See the "Related Topics" section on page 15-13.

System Requirements for Cisco WebDialer

Cisco WebDialer requires the following software components:

- Cisco CallManager 5.0(1) or later
- Cisco IP phone models that are supported by CTI

To configure your company directory search window for Cisco WebDialer or the Cisco CallManager directory search window, you must

- Install and configure Cisco CallManager.
- Configure Cisco WebDialer.

You can launch Cisco WebDialer from the Directory window, in Cisco CallManager User Options. You can access Cisco WebDialer from Cisco CallManager User Options, under the Directory link. For example, you could access a URL similar to the following one:

https://<ccmIP address>:8443/ccmuser

For documentation on installing and configuring Cisco CallManager, refer to the "Related Topics" section on page 15-13.

Interactions and Restrictions

The following sections describe the interactions and restrictions for Cisco WebDialer:

- Interactions, page 15-3
- Restrictions, page 15-4

Interactions

The following interactions apply to Cisco WebDialer:

- When using Client Matter Codes (CMC), the user must enter the proper code at the tone; otherwise, the IP phone disconnects, and the user receives reorder tone.

- When using Forced Authorization Codes (FMC), the user must enter the proper code at the tone; otherwise, the IP phone disconnects, and the user receives reorder tone.
- Cisco WebDialer uses change notifications on the ApplicationDialRule database table to track and use the updated dial rules.

Restrictions

Cisco WebDialer supports Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) based phones that Cisco Computer Telephony Integration (CTI) supports.

Note Cisco WebDialer supports only the 7970/71 and 7961/41 SIP IP phone models.

Additional Information

See the "Related Topics" section on page 15-13.

Installing and Activating Cisco WebDialer

Cisco WebDialer automatically installs on the server on which you installed Cisco CallManager.

Perform the following procedure to activate Cisco WebDialer on the Cisco CallManager server.

Procedure

Step 1 From the navigation area of the Cisco CallManager application, choose **Serviceability** and click **Go**.

Step 2 Choose **Tools** > **Service Activation**.

Step 3 Choose the Cisco CallManager server that is listed in the **Servers** drop-down list box.

Step 4 From CTI Services, check the check box next to **Cisco WebDialer Web Service**.

Step 5 Click **Save**.

Note You must also activate and start the CTI Manager service for Cisco WebDialer to function properly. To ensure that the CTI Manager service is started, from **CCM Serviceability**, choose **Tools >Control Center - Feature Services**.

Additional Information

See the "Related Topics" section on page 15-13.

Configuring Cisco WebDialer

This section contains the following information:

- Cisco WebDialer Configuration Checklist, page 15-5
- Configuring the Webdialer Servlet, page 15-6
- Setting Service Parameters for the Webdialer Servlet, page 15-6
- Configuring the Application User, page 15-7
- Configuring WebDialer for the Local Language, page 15-8
- Configuring the Redirector Servlet (Optional), page 15-9

Additional Information

See the "Related Topics" section on page 15-13.

Cisco WebDialer Configuration Checklist

Table 15-1 provides a configuration checklist for Cisco WebDialer. For more information, see the "Related Topics" section on page 15-13.

Table 15-1 Cisco WebDialer Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Activate the Cisco WebDialer service.	Installing and Activating Cisco WebDialer, page 15-4
Step 2	Configure the Webdialer servlet.	Setting Service Parameters for the Webdialer Servlet, page 15-6
Step 3	Add each user that you want to use WebDialer to the Standard End User Group for Cisco CallManager.	Adding Users to the Standard Cisco CallManager End Users Group, page 15-10
Step 4	Determine which language WebDialer displays by setting the locale field in the Cisco CallManager User Options Menu.	Configuring WebDialer for the Local Language, page 15-8
Step 5	(Optional) Configure the Redirector servlet.	Configuring the Redirector Servlet (Optional), page 15-9
Step 6	(Optional) Configure the application dial rules for multiple cluster applications.	Configuring Application Dial Rules (Optional), page 15-10
Step 7	(Optional) Create a proxy user.	Creating a Proxy User (Optional), page 15-11
Step 8	(Optional) Configure Cisco WebDialer trace settings.	Trace Settings (optional), page 15-12 *Cisco CallManager Serviceability Administration Guide*
Step 9	Configure Cisco WebDialer alarms.	Related Topics, page 15-13 *Cisco CallManager Serviceability Administration Guide*

Configuring the Webdialer Servlet

To configure the Webdialer servlet

- Activate the Cisco WebDialer service. See the "Installing and Activating Cisco WebDialer" section on page 15-4.
- Set trace settings (optional). See the "Trace Settings (optional)" section on page 15-12.
- Set the Cisco WebDialer service parameters. See the "Setting Service Parameters for the Webdialer Servlet" section on page 15-6.
- Configure application user.

Additional Information

See the "Related Topics" section on page 15-13.

Setting Service Parameters for the Webdialer Servlet

Cisco CallManager provides the following service parameters for the Webdialer Servlet:

- List of WebDialers—This parameter lists IP addresses for all WebDialers in your corporation. To enter new values, enter the IP address and port number of the Cisco CallManager server on which Cisco WebDialer is enabled.

  Ensure that a space separates each IP address and that only one WebDialer servlet per cluster is enabled. If more than one WebDialer servlet per cluster is enabled, a drop-down menu on the computer screen displays when the user clicks the telephone number of the person that the user wants to call.

  This drop-down menu contains the different locations where the calling party (end user making the call) is located. The end user chooses the appropriate location and proceeds to make the call.

Note Cisco CallManager Administration 5.0 requires that you specify a port number, for example, "172.19.253.97:8443" with "8443" as the port number.

- Primary Cisco CTIManager—Enter the IP address of the primary Cisco CTIManager.

  The default IP address of the Cisco CTI Manager specifies 127.0.0.1, which is the local host server that is used to set up Cisco WebDialer.

  The maximum length specifies 15 digits.
- Backup Cisco CTIManager—Enter the IP address of the backup Cisco CTIManager. The maximum length specifies 15 digits. No IP address implies that no backup CTI Manager exists.
- Duration of End Call Dialog (in seconds)—Enter the duration, in seconds, to display the dialog to end a call. This dialog indicates that the user must end the call if the user dialed out in error.

  The default value specifies 15 seconds, with a maximum value of 60 seconds and a minimum value of 10 seconds.
- User Session Expiry (in hours)—Enter the duration, in hours, for which the user login session is valid.

  A default value of 0 indicates that the login session is valid for an indefinite time, until Cisco WebDialer Web Service is restarted the next time.

  The minimum length specifies 0 hours, and the maximum length specifies 168 hours.

- Apply Application Dial Rules on Dial—Default specifies True. If you do not need Cisco WebDialer to use application dial rules, change the setting to False.
- CTI Manager Connection Security Flag—This clusterwide parameter indicates whether security for the Cisco WebDialer service CTI Manager connection gets enabled or disabled. If enabled, Cisco WebDialer opens a secure connection to CTI Manager by using the Application CAPF profile that is configured in Application CAPF Profile Instance Id for Secure Connection to CTI Manager parameter.
- CAPF Profile InstanceID for Secure Connection to CTI Manager—This parameter specifies the Instance Id of the Application CAPF Profile for Application User WDSecureSysUser that this Cisco WebDialer server will use to open a secure connection to CTI Manager.

Note All changes require a restart of the Cisco WebDialer service for the changes to take effect.

Use the following procedure to initially set or modify existing service parameters for the Webdialer servlet.

Procedure

Step 1 Choose **System** > **Service Parameters**.

Step 2 From the Server drop-down list box, choose the Cisco CallManager server on which you want to configure Cisco WebDialer service parameters.

Step 3 From the Service drop-down list box, choose the Cisco WebDialer Web Service.

Default values already exist for the parameters Primary Cisco CTIManager, Duration of End Call Dialog, User SessionExpiry (InHours), and Apply Application Dial Rules (True). Enter new values if your application requires them.

The parameter Backup Cisco CTIManager does not have any default values that are assigned to it. Enter values for this parameter if your application requires a backup Cisco CTIManager.

Step 4 For new parameter values to take effect, restart the Cisco WebDialer Web Service.

Additional Information

See the "Related Topics" section on page 15-13.

Configuring the Application User

The WebDialer needs a CTI connection to make and end calls. The WebDialer uses the application user and password that are required to create a CTI provider. (The database stores this value as application user and the system retrieves it from there.) To secure a TLS connection to CTI, see the "Secure TLS Connection to CTI" section on page 15-7.

Secure TLS Connection to CTI

Cisco WebDialer supports a secure (TLS) connection to CTI. Obtain the secure connection by using the "WDSecureSysUser" application user.

Note You must configure a CAPF profile, in the Application User CAPF Profile Configuration windows in Cisco CallManager Administration, that is configured for the instance ID for application user WDSecureSysUser to obtain a secure connection. If you enable security from the service parameters window, the Cisco WebDialer will open a secure connection to CTI Manager by using the Application CAPF profile. You should configure both the "CTI Connection Security Flag" and the "CAPF Profile InstanceID for Secure Connection to CTI Manager" service parameters for the secure connection to succeed. Refer to "Application User CAPF Profile Configuration" and "Service Parameters Configuration" in the *Cisco CallManager Administration Guide*.

Perform the following procedure to configure the application user.

Procedure

Step 1 Choose **User Management > Application User**.

The Find and List Application Users window displays.

Step 2 Click **Find**.

Step 3 From the Application User Configuration window, click **WDSysUser** or **WDSecureSysUser**.

Note To configure a CAPF profile, refer to "Application User CAPF Profile Configuration" in the *Cisco CallManager Administration Guide*.

Note You can change the password that is associated with the WDSysUser. The application obtains the new password from the database.

Additional Information

See the "Related Topics" section on page 15-13.

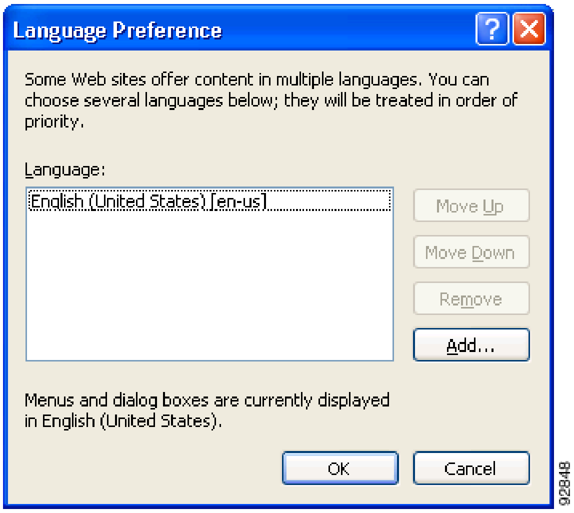
Configuring WebDialer for the Local Language

Cisco CallManager gives precedence to languages that are set up in the client browser; for example, Microsoft Internet Explorer (see Figure 15-1). To change the language that the client displays, use the browser settings (not the Locale field in the Cisco CallManager User Options menu). Conversely, Cisco WebDialer gives precedence to the locale that is configured in the Cisco CallManager User Options menu. Cisco WebDialer accesses locales in the following ways:

- You can configure a Cisco WebDialer user for a locale from the Cisco CallManager User Options Menu; for example, Japanese. When the user logs in to WebDialer, the WebDialer preferences window displays in Japanese. The user can change the language to the browser language; for example, by using Microsoft Internet Explorer. Cisco WebDialer recognizes the browser language only in the format ll_CC. For example, the Japanese locale gets defined as ja_JP.

- You can configure a Cisco WebDialer user for no locale (Locale field is set to None in the Cisco CallManager User Options menu). When the user logs in to WebDialer, the WebDialer preferences window displays in English. To change the language of the browser, the user must add a user-defined locale in the browser (using the format of ll_CC). For example, the Japanese locale gets defined as ja_JP.

Figure 15-1 Locale Settings in Microsoft Internet Explorer



Some Web sites offer content in multiple languages. You can choose several languages below; they will be treated in order of priority.

Language:

English (United States) [en-us]

Menus and dialog boxes are currently displayed in English (United States).

Refer to the documentation that came with your browser for information on how to change a user-defined locale. Refer to the *Customizing Your Cisco IP Phone on the Web* for information on how to set the locale in the Cisco CallManager User Options menu.

Additional Information

See the "Related Topics" section on page 15-13.

Partition Support

Cisco WebDialer includes partition information, provided by JTAPI, as well as line information. The following list comprises the different available configurations:

- Lines with the same DN: Cisco WebDialer handles different partition as different lines.
- Lines with the same DN: Cisco WebDialer handles same partition and different devices as shared lines.
- Lines with the same DN: Cisco WebDialer does not support same partition and in same device.

Additional Information

See the "Related Topics" section on page 15-13.

Configuring the Redirector Servlet (Optional)

Configure the Redirector servlet only if your applications require multiple clusters. Perform the following procedure to configure the Redirector servlet.

Procedure

Step 1 Choose **System > Service Parameters**.

Step 2 From the Server drop-down list box, choose the Cisco CallManager server on which you want to configure the Redirector Servlet.

Step 3 From the Service drop-down list box, choose the Cisco WebDialer Web Service.

Step 4 For the parameter, *List of WebDialers*, enter new values that your application requires. See the "Setting Service Parameters for the Webdialer Servlet" section on page 15-6 for a description of this service parameter.

Additional Information

See the "Related Topics" section on page 15-13.

Configuring Application Dial Rules (Optional)

Ensure that the application dial rules are configured for multiple cluster applications of Cisco WebDialer.

For information on configuring these application dial rules, refer to the "Application Dial Rules Configuration" section on page 29-1 in the *Cisco CallManager Administration Guide* for dial rule design and error checking.

Note Cisco WebDialer must pick up the dial rule change without a restart.

Additional Information

See the "Related Topics" section on page 15-13.

Adding Users to the Standard Cisco CallManager End Users Group

For users to use the Cisco WebDialer links in the User Directory windows in Cisco CallManager, you must add each user to the Standard Cisco CallManager End Users Group. The following procedure describes how to add users to this group.

Procedure

Step 1 Choose **User Management > User Group**.

The Find and List User Group window displays.

Click **Find**.

Step 2 Click the **Standard CCM End Users** link.

Step 3 The User Group Configuration window displays.

Step 4 Click **Add End Users to Group**.

The Find and List Users window displays.

Step 5 Click **Find**. You can enter criteria for a specific user.

Step 6 Check the check box next to the users that you want to add to the user group and click **Add Selected**.

Note If you want to add all users in the list of users, click **Select All** and then **Add Selected**.

The users display in the Users in Group table on the User Group Configuration window.

Additional Information

See the "Related Topics" section on page 15-13.

Creating a Proxy User (Optional)

Create a proxy user if you are using the makeCallProxy HTML over HTTP interface to develop an application for using Cisco WebDialer. For information on the makeCallProxy interface, refer to the *makeCallProxy* section in the *Cisco WebDialer API Reference Guide*.

You can enable authentication proxy rights for either an existing user or a new user.

Authentication Proxy Rights for Existing User

Perform the following procedure to enable authentication proxy rights for an existing user.

Procedure

Step 1 Choose **User Management** > **User Group**.

The Find and List User Group window displays.

Click **Find**.

Step 2 Click the **Standard EM Authentication ProxyRights** link.

The User Group Configuration window displays.

Step 3 Click **Add End Users to Group**.

The Find and List Users window displays.

Click **Find**. You can also add a criteria for a specific user.

Step 4 Choose the user to which you want to add proxy rights and click **Add Selected**.

Note If you want to add all the users in the list, click **Select All** and then click **Add Selected**.

The user displays in the Users in Group table on the User Configuration window.

Authentication Proxy Rights for New User

Perform the following procedure to enable authentication proxy rights for a new user.

Procedure

Step 1 Choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 Enter the following mandatory fields:

Last Name; **User ID**; **Password**; **Confirm Password**; **PIN**; and **Confirm PIN**.

Step 4 Click **Save**.

Step 5 Choose **User Management** > **User Group**.

The Find and List User Group window displays.

Step 6 Click the **Standard EM Authentication ProxyRights** link.

The User Group Configuration window displays.

Step 7 Click **Add End Users to Group**.

The Find and List Users window displays.

Step 8 Click **Find**. You can also enter criteria for a specific user.

Step 9 Choose the user to which you want to add proxy rights and click **Add Selected**.

Note If you want to add all the users in the list, click **Select All** and then click **Add Selected**.

The user displays in the Users in Group table on the User Configuration window.

Additional Information

See the "Related Topics" section on page 15-13.

Trace Settings (optional)

You can configure trace settings from Cisco CallManager Serviceability Administration. Find the traces at

/var/log/active/tomcat/logs/webdialer/log4j

/var/log/active/tomcat/logs/redirector/log4j

You can use the Real-Time Monitoring Tool (RTMT) to collect traces.

Note The same trace settings apply to both Cisco WebDialer and Redirector.

Perform the following procedure to enable debug traces for Cisco WebDialer.

Procedure

Step 1 From the navigation drop-down list box of the Cisco CallManager application, choose **Serviceability** and then click **Go**.

Step 2 Choose **Trace > Configuration**.

Step 3 From the Server drop-down list box, choose the server on which you want to enable traces for Cisco WebDialer.

Step 4 From the Service drop-down list box, choose the **Cisco WebDialer Web Service**.

Step 5 In the Trace Configuration window, change the trace settings according to your troubleshooting requirements. For more information on traces, refer to the *Cisco CallManager Serviceability Administration Guide.*

Step 6 Click **Save**.

Additional Information

See the "Related Topics" section on page 15-13.

Related Topics

- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Application Dial Rules Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Release 5.0*—A suite of documents that relate to the installation and configuration of Cisco CallManager. Refer to the *Cisco CallManager Documentation Guide for Release 5.x* for a list of documents on installing and configuring Cisco CallManager 5.x.
- *Cisco IP Phones and Services*—A suite of documents that relate to the installation and configuration of Cisco IP Phones.

CHAPTER 16

Cisco CallManager Attendant Console

Cisco CallManager Attendant Console, a client-server application, allows you to use a graphical user interface containing 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, or another employee can use it to manage his own telephone calls.

The attendant console installs on a PC with IP connectivity to the Cisco CallManager system. The attendant console works with a Cisco IP Phone that is registered to a Cisco CallManager system. Multiple attendant consoles can connect to a single Cisco CallManager system. When a server fails, the attendant console automatically connects to another server in the cluster.

The application registers with and receives call-dispatching, login, line state, and directory services from the Cisco CallManager Attendant Console Server service on the Cisco CallManager server. Cisco CallManager Attendant Console receives calls that are made to a virtual directory number that is called a pilot point and directs calls to a list of destinations in a hunt group. You can configure the order in which members of the hunt group receive calls and whether Cisco CallManager Attendant Console queues calls when all attendants are busy.

This section contains the following topics:

- Introducing Cisco CallManager Attendant Console, page 16-1
- System Requirements for Cisco CallManager Attendant Console, page 16-12
- Interactions and Restrictions, page 16-13
- Installing and Activating Cisco CallManager Attendant Console, page 16-15
- Configuring Cisco CallManager Attendant Console, page 16-15
- Dependency Records, page 16-38
- Troubleshooting Cisco CallManager Attendant Console, page 16-38
- Related Topics, page 16-39

Introducing Cisco CallManager Attendant Console

The following sections provide information about the Cisco CallManager Attendant Console feature:

- Understanding Cisco CallManager Attendant Console Users, page 16-2
- Understanding Pilot Points and Hunt Groups, page 16-2
- Understanding Call Queuing, page 16-9

- Understanding the Cisco CallManager Attendant Console Directory, page 16-9
- Understanding the Cisco CallManager Attendant Console Server, page 16-10
- Cisco CallManager Attendant Console Redundancy, page 16-11

Understanding Cisco CallManager Attendant Console Users

Before a user can log in to an attendant console to answer and direct calls, you must add the user as an attendant console user and optionally assign a password to the user. You can add or delete attendant console users and modify user IDs and password information in the Cisco CallManager Attendant Console User Configuration window in Cisco CallManager Administration.

Note Be aware that attendant console user IDs and passwords are not the same as directory users and passwords that are entered in the End User Configuration window in Cisco CallManager Administration.

If a user cannot log in to the attendant console, make sure that Cisco CallManager and Cisco CallManager Attendant Console Server services are both running. Verify that the user has been added in the Cisco CallManager Attendant Console User Configuration area of Cisco CallManager Administration and that the correct user name and password are specified in the Login dialog box in the attendant console client application.

In addition to configuring Cisco CallManager Attendant Console users, you must configure one directory user who is named “ac” and associate the attendant phones and the pilot points with the user. If you do not configure this user, the attendant console cannot interact with CTIManager. For information on setting up the ac user in Cisco CallManager Administration, see the “Configuring the ac User” section on page 16-20.

Understanding Pilot Points and Hunt Groups

A pilot point, a virtual directory number that is never busy, alerts the Cisco CallManager Attendant Console to receive and direct calls to hunt group members. A hunt group comprises a list of destinations that determine the call redirection order.

Note Cisco CallManager Attendant Console does not route calls to an instance of a shared line on attendant phone if any other instances of the shared line are in use.

For Cisco CallManager Attendant Console to function properly, make sure that the pilot point number is unique throughout the system (it cannot be a shared line appearance). When configuring the pilot point, you must choose one of the following routing options:

- First Available Hunt Group Member—Cisco CallManager Attendant Console goes through the members in the hunt group in order until it finds the first available destination for routing the call. You can choose this routing option from the Pilot Point Configuration window in Cisco CallManager Administration.
- Longest Idle Hunt Group Member—This feature arranges the members of a hunt group in order from longest to shortest idle time. Cisco CallManager Attendant Console finds the member with the longest idle time and, if available, routes the call. If not, Cisco CallManager Attendant Console

continues to search through the group. This feature evenly distributes the incoming call load among the members of the hunt group. You can choose this routing option from the Pilot Point Configuration window in Cisco CallManager Administration.

If the voice-mail number is the longest idle member of the group, Cisco CallManager Attendant Console routes the call to a voice-messaging system without checking the other members of the group first.

- Circular Hunting—Cisco CallManager Attendant Console maintains a record of the last hunt group member to receive a call. When a new call arrives, Cisco CallManager Attendant Console routes the call to the next hunt group member in the hunt group.
- Broadcast Hunting—When a call arrives at the pilot point, Cisco CallManager Attendant Console answers the call, places the call on hold, adds the call to the queue, and displays the call in the Broadcast Calls window on attendant PCs. While on hold, the caller receives music on hold, if it is configured. Any attendant can answer the call from the Broadcast Calls window.

Note In the Pilot Point Configuration window in Cisco CallManager Administration, you must choose a device pool that is associated with the pilot point for pilot point redundancy to work.

Make sure that you configure the ac user and associate all pilot point numbers with the ac user.

When you update a pilot point, make sure that you reset the pilot point. Call processing continues to occur when you reset it.

When a call comes into a pilot point, Cisco CallManager Attendant Console uses the hunt group list and the selected call routing method for that pilot point to determine the call destination. During hunt group configuration, you must specify one of the following options for each hunt group member:

- Directory number (device member)

  If a directory number is specified, Cisco CallManager Attendant Console only checks whether the line is available (not busy) before routing the call.
- Attendant console user plus a line number (user member)

  When you specify a user and line number, the user can log in to and receive calls on any Cisco IP Phone in the cluster that the attendant console controls.

  If a user and line number are specified, Cisco CallManager Attendant Console confirms the following details before routing the call:

  - That the user is logged in to the attendant console
  - That the user is online
  - That the line is available

  The attendant can only answer calls on the line number that you specify if that line number is configured on the phone that the attendant used to log in to the attendant console.

Caution To handle overflow conditions, configure your hunt groups, so Cisco CallManager Attendant Console route calls to one or more attendant consoles or voice-messaging numbers. To ensure that the voice-messaging number can handle more than one call at a time, check the Always Route Member check box in the Hunt Group Configuration window.

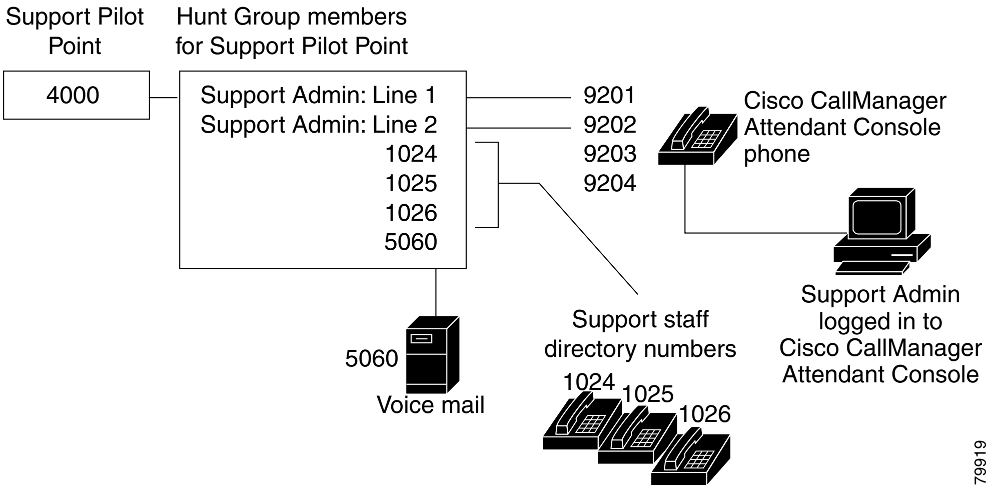
You can also handle overflow conditions by enabling call queuing. For more information about call queuing, see "Understanding Call Queuing" section on page 16-9.

Example 1 Pilot Points and Hunt Groups Working Together

Assume a pilot point named Support exists at directory number 4000. The hunt group for the Support pilot point contains the following members:

- Support Admin, Line 1 and Support Admin, Line 2 (Support Admin represents the attendant console login for the administrative assistant for Support.)
- Three directory numbers for support staff; that is, 1024, 1025, and 1026, listed in the hunt group in that order
- A voice-messaging number, 5060, which is the final member of the hunt group

Figure 16-1 Pilot Point and Hunt Group Example


Support Pilot Point
Hunt Group members for Support Pilot Point
4000
Support Admin: Line 1
Support Admin: Line 2
1024
1025
1026
5060
9201
9202
9203
9204
Cisco CallManager Attendant Console phone
Support Admin logged in to Cisco CallManager Attendant Console
Support staff directory numbers
1024
1025
1026
5060
Voice mail
79919

As shown in Figure 16-1, the following example describes a simple call-routing scenario where the user chose First Available Hunt Member during the configuration of the pilot point:

1. The Cisco Cisco CallManager Attendant Console receives a call and directs it to the Support Pilot Point, directory number 4000.
2. Because 4000 is a pilot point and First Available Hunt Group Member is chosen as the call-routing option, the Cisco CallManager Attendant Console that is associated with the pilot point checks the members of the hunt group in order, beginning with Support Admin, Line 1. Cisco CallManager Attendant Console determines that the Support Admin user is not online, directory number 1024 is busy, directory number 1025 is busy, and directory number 1026 is available.
3. Cisco CallManager Attendant Console routes the call to the first available directory number, which is 1026. Because 1026 is available, the Cisco CallManager Attendant Console never checks the 5060 number.

Understanding Linked Hunt Groups

Linking hunt groups together allows the Cisco CallManager Attendant Console to search through more than one hunt group when calls are routed. When configured properly, pilot points create a link between hunt groups. Cisco CallManager Attendant Console searches each hunt group according to the call-routing method that was chosen during configuration.

Consider the following guidelines when you are linking hunt groups together:

- Configure the individual pilot points and hunt groups first.
- For all except the last hunt group, make sure that the final member of the hunt group is the pilot point for the next hunt group. The pilot point from each group creates a link between the hunt groups, as seen in Figure 16-2.
- To handle overflow conditions, choose a voice-messaging or auto-attendant number as the final member of the last linked hunt group in the chain. If Cisco CallManager Attendant Console cannot route the call to any other members in the hunt groups, the call goes immediately to the voice-messaging number in the final hunt group.
- Check the Always Route Member check box in the Hunt Group Configuration window for only the final member of each hunt group.

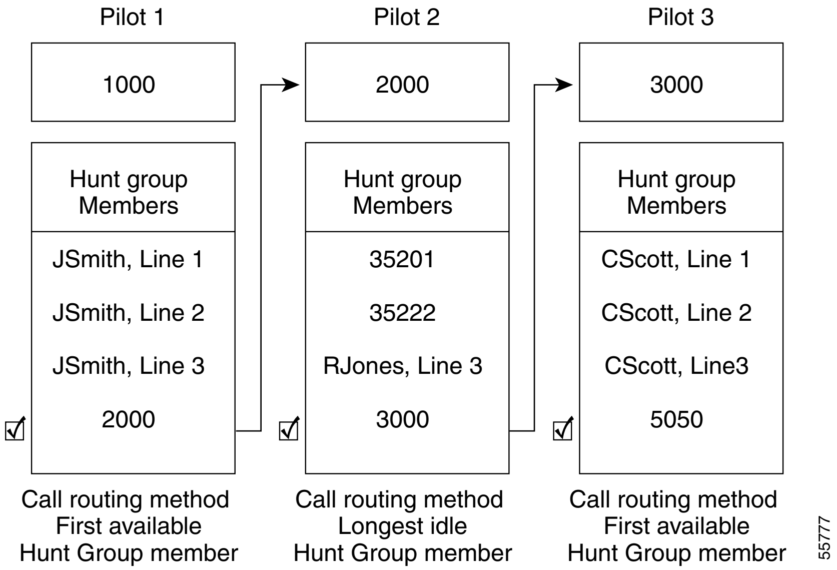
Caution Cisco strongly recommends that you do *not* link the last hunt group back to the first hunt group.

Example 2 Linked Hunt Groups Working Together

Consider the following information that is shown in Figure 16-2:

- Three pilot points that are numbered 1, 2, and 3 exist at directory numbers 1000, 2000, and 3000, respectively.
- The last hunt group member of Pilot 1 acts as the pilot point for Pilot 2, while the last hunt group member of Pilot 2 serves as the pilot point for Pilot 3.
- During hunt group configuration, the administrator checked Always Route Member for the last member of each hunt group.
- Each hunt group contains four members, including the linked pilot point.
- JSmith, RJones, and CScott designate attendant console users that are specified as user/line pairs in the hunt groups.
- In Pilot 2, two directory numbers, 35201 and 35222, exist.
- The final hunt group member of Pilot 3, voice-messaging number 5050, handles overflow conditions. The administrator checked Always Route Member when he configured this final hunt group member.

Figure 16-2 Linked Hunt Group Example



As represented in Figure 16-2, the following example describes a simple call- routing scenario for linked hunt groups:

1. The Cisco CallManager Attendant Console receives a call and directs it to the first pilot point of the chain, directory number 1000.
2. Because 1000 is a pilot point and First Available Hunt Group Member is chosen as the call-routing method, Cisco CallManager Attendant Console checks the members in the hunt group in order, beginning with JSmith, Line 1. Cisco CallManager Attendant Console determines that the first three members of the hunt group are unavailable and, therefore, routes the call to directory number 2000, the link to Pilot 2.
3. When the call reaches Pilot 2, Cisco CallManager Attendant Console attempts to route the call to the longest idle hunt group member. Because directory numbers 35201 and 35222 are busy, and RJones, Line 3, is offline, Cisco CallManager Attendant Console routes the call to the last member of the group, directory number 3000, the link to Pilot 3.
4. Cisco CallManager Attendant Console searches through Pilot 3 to find the first available member who is not busy. When Cisco CallManager Attendant Console determines that CScott, Line 2, is the first available member, Cisco CallManager Attendant Console routes the call to that line.
   Cisco CallManager Attendant Console never checks voice-messaging number 5050.

Understanding Circular Hunt Groups

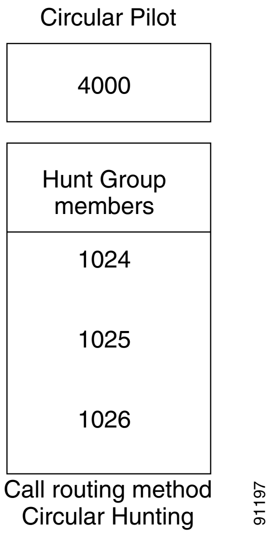
Circular hunt groups enable Cisco CallManager Attendant Console to route calls on the basis of last hunt group member to receive a call. Each hunt group maintains a record of which hunt group member receives a call. When a new call arrives, Cisco CallManager Attendant Console dispatches the call to the next hunt group member in the hunt group. In other words, Cisco CallManager Attendant Console routes the first call to a hunt group to the first hunt group member, the second call to the second hunt group member, and so on. After the last hunt group member receives a call, Cisco CallManager Attendant Console routes calls beginning with the first hunt group member again.

If you want to use circular hunting for linked hunt groups, set each of the pilot points of the linked hunt groups to circular hunting.

Example 3 Circular Hunting

Assume a pilot point that is named Circular exists at directory number 4000 and that you chose the Circular Hunting routing algorithm when you configured the pilot point. The hunt group for this pilot point contains the three directory numbers; that is, 1024, 1025, and 1026, listed in the hunt group in that order. Because the Always Route check box is not checked for any of the hunt group members, Cisco CallManager Attendant Console determines whether the directory number is busy before routing the call.

Figure 16-3 Circular Hunting Example



As shown in Figure 16-3, the following example describes a simple call-routing scenario where the user configured a Circular pilot point:

1. The Cisco CallManager Attendant Console receives a call and directs it to the Circular pilot point, directory number 4000.
2. Because 4000 is a pilot point and Circular Hunting is chosen as the call-routing option, Cisco CallManager Attendant Console routes the call to the first hunt group member, which is directory number 1024.
3. Cisco CallManager Attendant Console receives another call and directs it to the Circular pilot point, directory number 4000.
4. Because Circular Hunting is chosen as the call-routing option and directory number 1024 received the last call, Cisco CallManager Attendant Console attempts to route the call to the next hunt group member, which is directory number 1025.
5. Cisco CallManager Attendant Console determines that directory number 1025 is busy and routes the call to the next hunt group member, directory number 1026.
6. Cisco CallManager Attendant Console receives another call and directs it to the Circular pilot point, directory number 4000.
7. Because Circular Hunting is chosen as the call-routing option and directory number 1026 received the last call, Cisco CallManager Attendant Console attempts to route the call to the next hunt group member, which is directory number 1024.

Understanding Broadcast Hunting

Broadcast hunting enables Cisco Cisco CallManager Attendant Console to answer calls and place them into a queue. The attendant console displays the queued calls to all available attendants after inserting the calls into the queue and to all attendants that become available while the call is in the queue.

Note The attendant console only broadcasts calls to attendants that are set up as user/line number hunt group members in the broadcast hunting pilot point.

The queued calls appear in the Broadcast Calls window on the attendant PC. While in the queue, the callers receive music on hold if you have chosen an audio source from the Network Hold Audio Source and the User Hold MOH Audio Source drop-down list boxes in the Device Pool window or the Pilot Point Configuration window.

Any attendant in the hunt group that is online can answer the queued calls. Cisco CallManager Attendant Console does not automatically send the calls to an attendant. When an attendant answers a call, Cisco CallManager Attendant Console removes the call from the Broadcast Calls window and displays it in the Call Control window of the attendant who answered the call.

You can specify the following values for each broadcast hunting pilot point:

- Queue Size—This field specifies the number of calls that are allowed in the queue. If the queue is full, Cisco CallManager Attendant Console routes calls to the “always route” hunt group member that i s specified on the Hunt Group Configuration window. If you do not specify an always route member, Cisco CallManager Attendant Console drops the call when the queue size limit is reached.
- Hold Time—This field specifies the maximum time (in seconds) that Cisco CallManager Attendant Console keeps a call in the queue. If the call is in the queue for longer than the “HoldTime,” the call gets redirected to the “AlwaysRoute” member. If you do not configure an always route member, the call remains in the queue until an attendant becomes available.

Example 16-4 Broadcast Hunting Example

Assume a pilot point named Service exists at directory number 1000 and supports broadcast hunting. The hunt group for this pilot contains the following members:

- Three user/line number pairs for service staff; that is, Mary Brown/Line #1, Joe Williams/Line #2, and Doris Jones/Line #1, listed in the hunt group in that order
- A voice-messaging number, 7060, which is the final member of the hunt group

The following example describes a simple call-routing scenario where the user chose Broadcast Hunting during the configuration of the pilot point:

1. The Cisco CallManager Attendant Console receives a call and directs it to the Service Pilot Point, directory number 1000.
2. Because Broadcast is chosen as the call-routing option for the Service pilot point, the Cisco CallManager Attendant Console that is associated with the pilot point checks the queue. Cisco CallManager Attendant Console determines that the queue is not full and routes the call to the queue. The caller receives music on hold.

3. Cisco CallManager Attendant Console checks the members of the hunt group in order, beginning with Mary Brown/Line #1. Cisco CallManager Attendant Console determines that Mary Brown/Line #1 is available, Joe Williams/Line #2 is busy, and Doris Jones/Line #1 is available and, therefore, broadcasts the call to Mary Brown/Line #1 and Doris Jones/Line #1.
4. Mary Brown answers the call, and Cisco CallManager Attendant Console removes the call from the queue.

Understanding Call Queuing

You can configure a pilot point to support call queuing, so when a call comes to pilot point and all hunt groups members are busy, Cisco CallManager Attendant Console sends calls to a queue. While in the queue, the callers receive music on hold if you have chosen an audio source from the Network Hold Audio Source and the User Hold MOH Audio Source drop-down list boxes in the Device Pool window or the Pilot Point Configuration window. The attendants cannot view the queued calls. When a hunt group member becomes available, Cisco CallManager Attendant Console redirects the call to that hunt group member.

You enable queuing for a pilot point by checking the Queuing Enabled check box on the Pilot Point Configuration window. You must also enter a value in the Queue Size field and the Hold Time (in Seconds) field. The queue size specifies the number of calls that are allowed in the queue. If the queue is full, Cisco CallManager Attendant Console routes calls to the “always route” hunt group member that is specified on the Hunt Group Configuration window. If you do not specify an always route member, Cisco CallManager Attendant Console drops the call when the queue size limit is reached. The hold time specifies the maximum time (in seconds) that Cisco CallManager Attendant Console keeps a call in the queue. If the call is in the queue for longer than the “HoldTime,” the call gets redirected to “AlwaysRoute” member. If the “AlwaysRoute” member is not configured, no action occurs.

Understanding the Cisco CallManager Attendant Console Directory

The attendant console server reads and caches directory entries at startup. After an initial handshake determines whether the directory entries changed since the previous log in, the attendant console downloads the directory user list. The attendant console also downloads the user list when the interval in the Directory Reload Interval field in the Attendant Settings dialog box expires or when the user clicks the Reload button in the Directory window.

The attendant console searches the following files (in order) for the user list:

- User list file that is specified in the Path Name of Local Directory File in the Attendant Settings dialog box on the attendant PC
- AutoGenerated.txt file that is generated by the Cisco CallManager Attendant Console service and stored in the userlist directory on the Cisco CallManager Attendant Console server when the Cisco CallManager Attendant Console service starts and when the directory sync period expires if the Directory Sync Period service parameter does not equal zero. The attendant console saves the file as CorporateDirectory.txt.

  To modify the Directory Sync Period service parameter, choose **System > Service Parameters**. Choose the appropriate server from the Server drop-down list box and choose the Cisco CallManager Attendant Console Server service from the Service drop-down list box.
- CorporateDirectory.txt file that you import using the Cisco CM Attendant Console User File Upload window (**Application > Cisco CM Attendant Console > Cisco CM Attendant Console User File Upload**). If you import a CorporateDirectory.txt file, it replaces the AutoGenerated.txt file created by the system.

The user list file exists in comma separate value (CSV) format and contains the following information:

- Last Name
- First Name
- Telephone Number
- Department

Note Directory entries without telephone numbers do not display in the attendant console Directory window.

The attendant console server also stores per-attendant information such as speed-dial groups/entries and window positions in the database, which ensures that each attendant can use the per-attendant settings from any PC into which the attendant logs.

Additional Information

See the "Related Topics" section on page 16-39.

Understanding the Cisco CallManager Attendant Console Server

The attendant console application registers with and receives call-dispatching services from the Cisco CallManager Attendant Console Server service. The CallManager Attendant Console Server service provides communication among Cisco CallManager servers, attendant consoles, and the Cisco IP Phones that are used with the attendant consoles.

Note If you use the attendant console in a cluster environment, make sure that all Cisco CallManagers within a cluster have the Cisco CallManager Attendant Console Server service activated and running. You must manually activate the service through Cisco CallManager Serviceability. Attendant console redundancy requires this setup to work properly; however, not all Cisco CallManager Attendant Console Servers are required to have a route point.

Cisco CallManager Attendant Console Server handles attendant console requests for the following items:

- Call dispatching from pilot point to the appropriate hunt group destination
- Line status (unknown, available, on hook, or off hook)
- User directory information (Cisco CallManager Attendant Console Server stores and periodically updates directory information for fast lookup by the attendant console.)

Note Cisco CallManager Attendant Console Server only monitors the status of internal devices and phones. An attendant console user cannot see line state for a phone that is connected to a gateway.

Cisco CallManager Attendant Console Redundancy

Every time that the attendant opens the Cisco CallManager Attendant Console, the following events occur:

- Cisco CallManager Attendant Console connects to a Cisco CallManager Attendant Console server and downloads the list of Cisco CallManager servers in the attendant phone device pool.
- Cisco CallManager Attendant Console caches the list of servers into the GlobalSettings.xml file that is located in C:\Program Files\Cisco\Call Manager Attendant Console\data.
- Cisco CallManager Attendant Console client application uses the server list to locate the servers that are running CTIManager. The list of CTI services provides scalability. Customer can provision a single machine as the call processing server (CTI server) instead of running the CTI service on the same machine as the Cisco CallManager and the Attendant Console Server services.
- The Cisco CallManager Attendant Console server inspects the Cisco CallManager database and uses the list of Cisco CallManager servers as the list of servers where the Cisco CallManager Attendant Console Server service should be active.

If a Cisco CallManager service fails, the following events occur:

- The attendant console that is attached to the failed server uses the list in the GlobalSettings.xml file to locate and connect to another Cisco CallManager server.
- The Cisco CallManager Attendant Console Server service that is running on the Cisco CallManager server takes over servicing of the route points that are associated with the failed Cisco CallManager.
- When the failed Cisco CallManager comes back up, its Cisco CallManager Attendant Console Server resumes servicing its route points and attendant consoles. The attendants resumes service with the recovered Cisco CallManager after the attendant closes and reopens the console.

Note Automated recovery exists. If a Cisco CallManager Attendant Console Server service fails, another Cisco CallManager Attendant Console Server service takes over.

To ensure redundancy for the Cisco CallManager Attendant Console application, perform one of the following tasks:

- In default configurations where CTIManager and Cisco CallManager Attendant Console Server are running on all nodes in the Cisco CallManager cluster, enter the IP address of one server that is running Cisco CallManager Attendant Console Server in the Attendant Settings dialog box on the attendant PC.
- If Cisco CallManager Attendant Console Server and CTIManager are not running on all nodes in the cluster, enter a comma separated list of the IP addresses of servers in the cluster that have an active CTIManager in the Call Processing Server Host Names or IP Addresses field on the Advanced Tab of the Attendant Settings dialog box on the attendant PC.

Note For more information on accessing the Attendant Settings dialog box, see the "Configuring Cisco CallManager Attendant Console Settings" section on page 16-35.

System Requirements for Cisco CallManager Attendant Console

See the following sections for PC requirements and Cisco IP Phone requirements for using the attendant console:

- Attendant PC Requirements, page 16-12
- Cisco IP Phone and Voice-Messaging Requirements for Use with the Attendant Console, page 16-12

Attendant PC Requirements

The following list provides PC requirements for the attendant console:

- Operating system—Windows 2000 and Windows XP
- Network connectivity to the Cisco CallManager

Cisco IP Phone and Voice-Messaging Requirements for Use with the Attendant Console

The attendant console works in conjunction with a Cisco IP Phone. Configure the attendant console to connect the Cisco IP Phone to its registered Cisco CallManager server. To configure the attendant console, make sure that the IP Address or Host Name field in the Attendant Console Settings dialog box specifies the address of the Cisco CallManager server to which the Cisco IP Phone is normally registered.

Cisco IP Phones that are used with the attendant console must meet the following guidelines:

- Use the attendant console with any SCCP Cisco IP Phone Models 7902, 7905, 7912, 7940, 7960, and 7970. You cannot use SIP phones as attendant phones, but attendants can receive and handle calls from SIP phones.
- Make sure that the Cisco IP Phone is added as a device in Cisco CallManager before it is used with the attendant console.
- Make sure that you associate the attendant directory numbers in addition to the pilot points and devices with the ac user that you configured in the Application User Configuration window in Cisco CallManager Administration.
- Make sure that you configure voice messaging for each directory number the attendant can access. If you do not, the attendant cannot forward calls to voice-messaging system.
- Do not use a shared-line appearance for pilot points. Make sure that directory numbers for pilot points do not appear on any other device in the system. Attendant phones can share lines with other attendants or non-attendants.
- Disable call forwarding for lines and directory numbers on Cisco IP Phones that are used as attendant consoles.
- If an attendant console user will be logging in to the attendant console at more than one phone, ensure that each phone is set up according to these guidelines and that each phone is registered with its own attendant console.

- Based on the line settings on Directory Number Configuration window, Cisco CallManager Attendant Console can support multiple calls on a line. When no more outgoing calls can be made on a line, Cisco CallManager Attendant Console displays a warning message when the attendant attempts to make a call.

Interactions and Restrictions

The following sections describe the interactions and restrictions for Cisco CallManager Attendant Console:

- Interactions, page 16-13
- Restrictions, page 16-14

Interactions

The following sections describe how Cisco CallManager Attendant Console interacts with Cisco CallManager applications:

- Cisco CallManager Extension Mobility, page 16-13
- Music On Hold, page 16-13
- Call Park, page 16-13
- CTI, page 16-14

Cisco CallManager Extension Mobility

If a user logs in to or logs off the Cisco IP Phone by using Cisco CallManager Extension Mobility while logged in to Cisco CallManager Attendant Console, the Cisco IP Phone resets, and the call-control status of the attendant console goes down. Cisco CallManager Attendant Console displays a message that indicates that the attendant needs to log out and log back in if the directory numbers of the phone have changed. The user must log out of the Cisco CallManager Attendant Console. When logging back into the Cisco CallManager Attendant Console, the attendant must specify the current directory number of the phone in the Directory Number of Your Phone field of the Settings dialog box.

For more information on entering a directory number in the Cisco CallManager Attendant Console, see "Configuring Cisco CallManager Attendant Console Settings" section on page 16-35.

Music On Hold

If you have chosen an audio source from the Network Hold Audio Source and the User Hold MOH Audio Source drop-down list boxes in the Device Pool window or on the Pilot Point window, queued callers receive music on hold while in the queue. The selections you make on the Pilot Point Configuration window override those you make on the Device Pool window.

Call Park

You must associate the ac user to the Standard CTI Allow Call Park Monitoring group (found on the Cisco CallManager Administration User Group Configuration window). If you do not associate the ac user to this group, pilot points do not register, and the call control does not go up on the console.

CTI

You must associate the ac user to the Standard CTI Enabled users group and the Standard CTI Allow Call Park Monitoring group (found on the Cisco CallManager Administration User Group Configuration window). If you do not associate the ac user to these groups, pilot points do not register, and the call control does not go up on the console.

Restrictions

The following restrictions apply to Cisco CallManager Attendant Console:

- You cannot use SIP phones as attendant phones, but attendants can receive and handle calls from SIP phones.
- The attendant console does not show the correct call forward all (CFA) status of certain SIP phones, including Cisco SIP IP Phone models 7940 and 7960.
- Cisco CallManager Attendant Console Server does not route calls to an instance of a shared line on attendant phone if any other instances of the shared line are in use.
- If you use the attendant console in a cluster environment, make sure that all Cisco CallManagers within a cluster have the Cisco CallManager Attendant Console Server service activated and running. You must manually activate the service through Cisco CallManager Serviceability. Attendant console redundancy requires this setup to work properly; however, not all Cisco CallManager Attendant Console Servers are required to have a route point.
- Cisco CallManager Attendant Console does not support a dual monitor setup on the attendant PC.
- Cisco CallManager Attendant Console does not support Barge and cBarge; however, the client interface does display any activity that is related to these features.
- Do not use a shared-line appearance for pilot points and hunt group members. Make sure that directory numbers for pilot points and hunt group members do not appear on any other device in the system.
- Disable call forwarding for lines and directory numbers on Cisco IP Phones that are used as attendant consoles.
- Cisco CallManager Attendant Console recognizes partitions, but has the following problems working with them:
  - If a directory number exists in more than one partition, the attendant console displays the line state of the DN that changed last. This means that line state that appears for a particular individual in the directory may not be correct.
  - If a directory number in the hunt group also exists in another partition, Cisco CallManager Attendant Console may not route calls appropriately. Consider a scenario in which directory number 2000 exists in Partition1 and Partition2, and directory number 2000 (Partition1) exists in a hunt group. If directory number 2000 (Partition2) receives a call, Cisco CallManager Attendant Console considers the line state of directory number 2000 (Partition1) to be busy and does not route calls to that directory number.
- A user cannot activate call back for a Cisco CallManager Attendant Console pilot point number over a QSIG-enabled intercluster trunk or QSIG-enabled trunk. If the user attempts to activate call back to a Cisco CallManager Attendant Console pilot point number over a QSIG-enabled intercluster trunk or QSIG-enabled trunk, the message “Callback Cannot be activated on xxxx” displays on the user phone. The user can activate call back for a Cisco CallManager Attendant Console pilot point if that pilot point exists in the same Cisco CallManager cluster as the user DN.

- Cisco CallManager Attendant Console does not work with the group call pickup feature. The attendant console user interface cannot appropriately handle calls coming from or made to phones belonging to a call pickup group due to JTAPI and CTI limitations.
- Make sure that you do not add attendant console pilot points or hunt group members or any directory numbers on an attendant phone to line groups in Cisco CallManager Administration.

Installing and Activating Cisco CallManager Attendant Console

1. Use Cisco CallManager Serviceability to activate and start the Cisco CallManager Attendant Console Server service on all servers that are running the Cisco CallManager service and to activate the CTIManager service on one server in the cluster. Refer to the *Cisco CallManager Serviceability Administration Guid*e.
2. Configure Cisco CallManager Attendant Console in Cisco CallManager Administration. See the "Configuring Cisco CallManager Attendant Console" section on page 16-15.
3. Install and configure the Cisco CallManager Attendant Console plug-in on each attendant PC. For more information, see the "Installing the Cisco CallManager Attendant Console Plug-in on an Attendant PC" section on page 16-33, the "Starting Cisco CallManager Attendant Console After Installing Windows XP SP2" section on page 16-34, and the "Configuring Cisco CallManager Attendant Console Settings" section on page 16-35. After the attendant console is configured, it operates with the specified settings until the administrator changes them.
4. If the attendants require Cisco Attendant Console user windows to display in a language other than English, make sure that you install the Cisco IP Telephony Locale Installer on every server in the cluster. For more information, refer to the *Cisco IP Telephony Platform Administration Guide*.

Configuring Cisco CallManager Attendant Console

For successful configuration of Cisco CallManager Attendant Console, perform the steps in the configuration checklist. The following sections provide configuration information:

- Configuration Checklist for Cisco CallManager Attendant Console, page 16-16
- Configuring Cisco CallManager Attendant Console Users, page 16-17
- Configuring the ac User, page 16-20
- Configuring Pilot Points, page 16-21
- Associating Devices and Pilot Points with the ac User, page 16-27
- Configuring Hunt Groups, page 16-28
- Cisco CallManager Attendant Console Server Configuration, page 16-31
- Creating and Uploading the CorporateDirectory.txt File, page 16-31
- Deleting the CorporateDirectory.txt File, page 16-33
- Installing the Cisco CallManager Attendant Console Plug-in on an Attendant PC, page 16-33
- Starting Cisco CallManager Attendant Console After Installing Windows XP SP2, page 16-34
- Configuring Cisco CallManager Attendant Console Settings, page 16-35
- Attendant Console Configuration Settings, page 16-35

- Configuring Held Icon Timers, page 16-37
- Dependency Records, page 16-38

Configuration Checklist for Cisco CallManager Attendant Console

Perform the steps in Table 16-1 to set up the attendant console.

Table 16-1 Attendant Console Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Add attendant console users.	Configuring Cisco CallManager Attendant Console Users, page 16-17
Step 2	Configure directory numbers for the pilot points.	Configuring a Directory Number, *Cisco CallManager Administration Guide*
Step 3	Set up pilot points and hunt groups.	Understanding Pilot Points and Hunt Groups, page 16-2 Configuring Pilot Points, page 16-21 Configuring Hunt Groups, page 16-28
Step 4	Create the ac user and associate all pilot point devices with the user.	Configuring the ac User, page 16-20 Associating Devices and Pilot Points with the ac User, page 16-27
Step 5	Add the ac user to the Standard CTI Enabled group and the Standard CTI Allow Call Park Monitoring group.	Adding Users to a User Group, *Cisco CallManager Administration Guide*.
Step 6	Verify that the Cisco CallManager Attendant Console Server service activates and runs on all servers that are running the Cisco CallManager service. Verify that the CTIManager service activates and runs on one server in the cluster.	*Cisco CallManager Serviceability Administration Guide* Understanding the Cisco CallManager Attendant Console Server, page 16-10
Step 7	Make sure that each attendant Cisco IP Phone is set up correctly for use with the attendant console.	Cisco IP Phone and Voice-Messaging Requirements for Use with the Attendant Console, page 16-12
Step 8	Make sure that the attendant console PC is set up correctly for use with the attendant console.	Attendant PC Requirements, page 16-12
Step 9	Create dial rules to transform directory numbers into a dialable pattern. Each rule specifies which numbers to transform based on the beginning digits and length of the number. For example, you can create a dial rule that automatically removes the area code and prefix digits from a 10-digit telephone number beginning with 408525 and adds 89 to the beginning of the telephone number to provide access to an outside line. In this case, the number 4085256666 becomes 8956666.	Configuring Dial Rules, *Cisco CallManager Administration Guide* Dial Rules Overview, *Cisco CallManager System Guide*

Table 16-1 Attendant Console Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 10	Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory. For example, you can create a directory lookup rule that automatically removes the area code and 2 prefix digits from a 10-digit telephone, which would transform 4089023139 into 23139. If Cisco CallManager Attendant Console can match the number with a user in the speed dial entries of the attendant or in the directory, the attendant console displays the name in the Call Detail window.	Configuring Directory Lookup Dial Rules, page 30-2, *Cisco CallManager Administration Guide* Directory Lookup Dial Rules, *Cisco CallManager System Guide*
Step 11	If your centralized user list is located on a directory server that is separate from the Cisco CallManager server, create and upload the CorporateDirectory.txt file.	Creating and Uploading the CorporateDirectory.txt File, page 16-31
Step 12	Install and configure the attendant console on each attendant console user PC. **Note** After a Cisco CallManager upgrade, you must reinstall the Cisco CallManager Attendant Console Plug-in on the attendant PCs.	Installing the Cisco CallManager Attendant Console Plug-in on an Attendant PC, page 16-33 Starting Cisco CallManager Attendant Console After Installing Windows XP SP2, page 16-34 Configuring Cisco CallManager Attendant Console Settings, page 16-35

Configuring Cisco CallManager Attendant Console Users

This section covers the following procedures:

- Finding an Attendant Console User, page 16-17
- Configuring an Attendant Console User, page 16-19
- Deleting an Attendant Console User, page 16-20
- Configuring the ac User, page 16-20

Additional Information

See the "Related Topics" section on page 16-39.

Finding an Attendant Console User

Use the following procedure to find an attendant console user:

Note During your work in a browser session, Cisco CallManager Administration retains your attendant console user search preferences. If you navigate to other menu items and return to this menu item, Cisco CallManager Administration retains your user search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Application** > **Cisco CM Attendant Console > Cisco CM Attendant Console User**.

The Find and List window displays.

Step 2 From the drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

Tip To find all attendant console users that are registered in the database, click **Find** without entering any search text.

A list of attendant console users displays by Name.

Tip To search for directory numbers within the search results, click the **Extend Query** check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Information

See the "Related Topics" section on page 16-39.

Configuring an Attendant Console User

This section describes how to configure an attendant console user. You must add users through the Cisco CallManager Attendant Console User Configuration window in Cisco CallManager Administration before the users can log in to an attendant console.

Note Be aware that attendant console user IDs and passwords are *not* the same as directory users and passwords that are entered in the End User Configuration window in Cisco CallManager Administration.

Procedure

Step 1 Choose **Application** > **Cisco CM Attendant Console** > **Cisco CM Attendant Console User**.

Step 2 Perform one of the following tasks:

- To add a new attendant console user, click the **Add New** button.
- To update an existing attendant console user, locate the appropriate user as described in "Finding an Attendant Console User" section on page 16-17, and click the name of the user you want to update.

The Cisco CallManager Attendant Console User Configuration window displays.

Step 3 Enter the appropriate configuration settings as described in Table 16-2.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 16-39.

Cisco CallManager Attendant Console User Configuration Settings

Table 16-2 describes Cisco CallManager Attendant Console user configuration settings.

Table 16-2 Attendant Console User Configuration Settings

Field	Description
User ID	Enter the login name for the attendant console user. Enter up to 50 alphanumeric characters.
Password	Enter a password of up to 50 alphanumeric characters.
Confirm	Enter the same password again.

Additional Information

See the "Related Topics" section on page 16-39.

Deleting an Attendant Console User

This section describes how to view, update, or delete a Cisco attendant console user.

Before You Begin

To find out which hunt groups are using the attendant console user, click the **Dependency Records** link from the Cisco CallManager Attendant Console User Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, refer to the "Accessing Dependency Records" section in the *Cisco CallManager Administration Guide*. If you try to delete an attendant console user that is in use, Cisco CallManager displays a message. To delete an attendant console user that is currently in use, you must perform either or both of the following tasks:

- Assign a different attendant console user to any hunt groups that are using the attendant console user that you want to delete. See the "Deleting Hunt Group Members" section on page 16-30.
- Delete the hunt groups that are using the attendant console user. See the "Deleting Hunt Group Members" section on page 16-30.

Procedure

Step 1 Locate the user you want to delete by using the procedure in the "Finding an Attendant Console User" section on page 16-17.

Step 2 Click the name of the user that you want to delete.

Step 3 To remove the user, click **Delete**.

Tip From the Find and List window, you can delete multiple users by checking the check boxes next to the appropriate users and clicking **Delete Selected**. You can delete all users in the window by clicking **Select All**, then clicking **Delete Selected**.

Additional Information

See the "Related Topics" section on page 16-39.

Configuring the ac User

You must configure one user named "ac" and associate the attendant phones and the pilot points with the user. If you do not configure this user, the attendant console cannot interact with CTIManager, and the attendant cannot receive calls.

Note After you use this procedure to create the ac user with the specified user ID and password, you can change the user ID and password. If you change the user ID, you must also change the JTAPI username field in the Service Parameters Configuration window for the Cisco CallManager Attendant Console Server service. For information on accessing the Cisco CallManager Attendant Console service parameters, see the "Cisco CallManager Attendant Console Server Configuration" section on page 16-31.

Perform the following procedure to configure the ac user.

Procedure

Step 1 Choose **User Management > Application User**.

The Find and List Application Users window displays.

Step 2 Click **Add New**.

The Application User Configuration window displays.

Step 3 In the User ID field, enter **ac**.

Step 4 In the Password field, enter **12345**.

Step 5 In the Confirm Password field, enter **12345**.

Step 6 Click **Save**.

Note If you want to change the ac user ID and password after the ac user has been created, use this procedure to change the values. If you change the user ID, you must also enter the new user ID in the JTAPI username field in the Service Parameters Configuration window for the Cisco CallManager Attendant Console Server service. For information on accessing the Cisco CallManager Attendant Console service parameters, see the "Cisco CallManager Attendant Console Server Configuration" section on page 16-31.

Additional Information

See the "Related Topics" section on page 16-39.

Configuring Pilot Points

Before the Cisco CallManager Attendant Console Server can route calls, you must configure pilot points and hunt groups through Cisco CallManager Administration.

Note After you configure the pilot points, make sure that you configure the ac user and associate all pilot points with the ac user.

This section contains the following topics:

- Finding a Pilot Point, page 16-22
- Configuring a Pilot Point, page 16-23
- Deleting a Pilot Point, page 16-26
- Resetting a Pilot Point, page 16-26
- Pilot Point Configuration Settings, page 16-24
- Associating Devices and Pilot Points with the ac User, page 16-27

Additional Information

See the "Related Topics" section on page 16-39.

Finding a Pilot Point

This section describes how to find a pilot point.

Note During your work in a browser session, Cisco CallManager Administration retains your pilot point search preferences. If you navigate to other menu items and return to this menu item, Cisco CallManager Administration retains your pilot point search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Application** > **Cisco CM Attendant Console** > **Pilot Point**.

The Find and List window displays.

Step 2 From the drop-down list box, choose one of the following criteria:

- Pilot Point
- Calling Search Space
- Device Pool
- Pilot Number
- Partition

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

Tip To find all pilot points that are registered in the database, click **Find** without entering any search text.

A list of pilot points displays.

Tip To search for a pilot point within the search results, click the **Extend Query** check box, enter your search criteria as described in this procedure, and click **Find**.

Step 4 To view a specific pilot point, click the pilot point name.

Step 5 To delete or reset multiple pilot points from the Find and List Pilot Points window, check the check boxes next to the appropriate pilot points. You can choose all the phones in the window by checking the **Select All** button. Then, do one of the following:

- To delete the pilot points, click **Delete Selected**. When the delete confirmation dialog box displays, click **OK**.
- To reset the pilot points, click **Reset Selected**. When the Device Reset window displays, click **Restart**.

Additional Information

See the "Related Topics" section on page 16-39.

Configuring a Pilot Point

This section describes how to configure a pilot point and how to associate the directory number with that pilot point.

Before You Begin

Configure directory numbers to associate with the pilot points.

For more information on configuring directory numbers, see the "Configuring a Directory Number" section in the *Cisco CallManager Administration Guide*.

Procedure

Step 1 Choose **Application** > **Cisco CM Attendant Console > Pilot Point**.

The Find and List Pilot Points window displays.

Step 2 Perform one of the followings tasks:

- To copy an pilot point, locate the appropriate phone as described in "Finding a Pilot Point" section on page 16-22, and click the **Copy** button.
- To add a new pilot point, click the **Add New** button.
- To update an existing phone, locate the appropriate phone as described in "Finding a Pilot Point" section on page 16-22.

Step 3 Enter the appropriate settings as described in Table 16-3.

Step 4 Click **Save**.

Step 5 To associate a directory number for the pilot point, click the **Line [1]** link.

The Directory Number Configuration window displays.

Step 6 Enter the directory number that you want to use for the pilot point from the Directory Number field and click **Save**.

Note After the pilot point is created, you must configure a hunt group to specify which attendants receive the calls that come in to the pilot point. For more information, see the "Configuring Hunt Group Members" section on page 16-28.

Tip After you configure the pilot points, remember to configure the ac user and associate the devices/pilot points with the ac user. See the "Configuring the ac User" section on page 16-20 and the "Associating Devices and Pilot Points with the ac User" section on page 16-27 for more information.

Additional Information

See the "Related Topics" section on page 16-39.

Pilot Point Configuration Settings

Table 16-3 describes pilot point configuration settings.

Table 16-3 Pilot Point Configuration Settings

Field	Description
Pilot Name	Enter up to 15 alphanumeric characters, including spaces, to specify a descriptive name for the pilot point.
Description	Enter a description of the pilot point. This description can contain up to 50 characters.
Device Pool	The device pool comprises a group of Cisco CallManagers in prioritized order. The first Cisco CallManager in the list represents the primary Cisco CallManager for the pilot point.
Calling Search Space	To designate the partitions that the pilot point searches when it attempts to route a call, choose a calling search space from the drop-down list. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the **Find** button displays next to the drop-down list box. Click the **Find** button to display the Select Calling Search Space window. Enter a partial calling search space name in the **List items where Name contains** field. Click the desired calling search space name in the list of calling search spaces that displays in the **Select item to use** box and click **OK**. **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and enter a value in the Max List Box Items field.
Route Calls To	Choose the method by which Cisco CallManager Attendant Console routes calls to attendants. The available methods include • First Available Hunt Group Member—Routes incoming calls to the first available member of a hunt group. • Longest Idle Hunt Group Member—Routes incoming calls to the route group member that has been idle for the longest time. If the voice-messaging number is the longest idle member of the group, Cisco CallManager Attendant Console routes the call to voice-messaging system without first checking the other members of the group. • Circular Hunting—Cisco CallManager Attendant Console maintains a record of the last hunt group member to receive a call. When a new call arrives, Cisco CallManager Attendant Console routes the call to the next hunt group member in the hunt group. • Broadcast Hunting—When a call arrives at the pilot point, Cisco CallManager Attendant Console answers the call, places the call on hold, adds the call to the queue, and displays the call in the Broadcast Calls window on attendant PCs. While on hold, the caller receives music on hold, if it is configured. Any attendant can answer the call from the Broadcast Calls window.
Location	This field specifies a selection of locations that are defined by using **System > Location**. When a location is defined, a location name, audio and video bandwidths get specified.

Table 16-3 Pilot Point Configuration Settings (continued)

Field	Description
Media Resource Group	Choose the appropriate Media Resource Group List. A Media Resource Group List specifies a prioritized list of media resource groups. Cisco CallManager Attendant Console selects the required media resource (for example, a Music On Hold server, transcoder, or conference bridge) from the available media resource groups according to the priority order that is defined in the media resource group list. **Note** For more information on media resource group lists, see "Configuring a Media Resource Group List" in the *Cisco CallManager Administration Guide*.
Network Hold MOH Audio Source	Choose the audio source that Cisco CallManager Attendant Console uses for network hold, including transfer hold, conference hold, and call park hold.
User Hold MOH Audio Source	Choose the audio source that Cisco CallManager Attendant Console uses when the attendant places a caller on hold.
Queuing Enable	If you want Cisco CallManager Attendant Console to queue calls when all attendants in a hunt group are busy, check the **Queuing Enable** check box. To complete the call-queuing configuration, enter values in the Queue Size and Queue Hold Time (in Seconds) fields.
Queue Size	This field specifies the number of calls that are allowed in the queue. If the queue is full, Cisco CallManager Attendant Console routes calls to the "always route" member that is specified on the Hunt Group Configuration window. If you do not specify an always route member, Cisco CallManager Attendant Console drops the call when the queue size limit is reached. The range is 0 to 255. The default specifies 32.
Queue Hold Time (in Seconds)	This field specifies the maximum time (in seconds) that Cisco CallManager Attendant Console keeps a call in the queue. If a call remains on hold for the number of seconds that are entered in this field and you configured an "always route" hunt group member on the Hunt Group Configuration window, Cisco CallManager Attendant Console sends the call to the always route member that is specified on the Hunt Group Configuration window. If you do not configure an always route member, the call remains in the queue until an attendant becomes available. Enter 0 in this field to keep calls in the queue until an attendant becomes available. The range is 0 to 3600 seconds. The default specifies 0.

Additional Information

See the "Related Topics" section on page 16-39.

Deleting a Pilot Point

This section describes how to delete a pilot point.

Before You Begin

To find out which virtual directory numbers are using the pilot point, click the **Dependency Records** link from the Pilot Point Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, refer to the "Accessing Dependency Records" section in the *Cisco CallManager Administration Guide*. If you try to delete a pilot point that is in use, Cisco CallManager displays a message. To delete a pilot point that is currently in use, you must delete the virtual directory numbers that are using the pilot point.

Note You do not have to restart Cisco CallManager Attendant Console Server or Cisco CallManager service after you delete a pilot point for the deletion to take effect.

Procedure

Step 1 Locate the pilot point by using the procedure in the "Finding a Pilot Point" section on page 16-22.

Step 2 Click the name of the pilot point that you want to delete. The Pilot Point Configuration window displays with information for the chosen pilot point.

Step 3 To remove the pilot point, click the **Delete** button.

Approximately 10 minutes after you delete a pilot point, Cisco CallManager Attendant Console stops directing calls to any hunt group members that are associated with that pilot point.

Tip From the Find and List window, you can delete multiple pilot points by checking the check boxes next to the appropriate pilot points and clicking **Delete Selected**. You can delete all pilot points in the window by clicking **Select All**, then clicking **Delete Selected**.

Additional Information

See the "Related Topics" section on page 16-39.

Resetting a Pilot Point

You must reset the pilot point after you update pilot point configuration settings. When you reset the pilot point, the Cisco CallManager service continues to run, and call processing continues to occur. Perform the following procedure to reset the pilot point:

Procedure

Step 1 Locate the pilot point that you want to reset by using the procedure in the "Finding a Pilot Point" section on page 16-22.

Step 2 Click the name of the pilot point that you want to reset.

Step 3 Click **Reset**.

The Reset window displays.

Step 4 Click one of the following buttons:

- **Restart**—Restarts the selected device for the pilot point without shutting the device down (reregisters the phones with Cisco CallManager).
- **Reset**—Shuts down the selected device for the pilot point and brings it back up (performs a complete shutdown and reinitialization of the phone).
- **Close**—Returns you to the previous window without restarting or resetting the selected device.

Additional Information

See the "Related Topics" section on page 16-39.

Associating Devices and Pilot Points with the ac User

Before the attendant uses the attendant console, you must associate the attendant console phones and pilot points to the ac user. Perform the following procedure:

Procedure

Step 1 Choose **User Management > Application User**, and perform a search for the ac user that you set up in the "Configuring the ac User" section on page 16-20. For more information on performing a user search, see the "Finding an End User" in the *Cisco CallManager Administration Guide*.

The ac user information appears in the Application User Configuration window.

Step 2 Choose the pilot points from the Available Devices list in the Device Associations box that you want to associate with the ac user and click the down arrow to move the pilot points to the Controlled Devices box. To choose multiple pilot points, Ctrl+click the pilot points. To locate specific pilot points, click the **Find More Pilot Points** button, locate the pilot points as described in "Finding a Pilot Point" section on page 16-22, check the check boxes next to the pilot points that you want to associate to the ac user, and click **Add Selected**.

Step 3 Click **Save**.

Additional Information

See the "Related Topics" section on page 16-39.

Configuring Hunt Groups

After you configure the pilot point, you must configure the hunt group. A hunt group comprises an ordered list of destinations (either directory numbers or attendant console user/line numbers) to which Cisco CallManager Attendant Console directs incoming calls.

This section covers the following procedures:

- Configuring Hunt Group Members, page 16-28
- Hunt Group Configuration Settings, page 16-29
- Deleting Hunt Group Members, page 16-30

Additional Information

See the "Related Topics" section on page 16-39.

Configuring Hunt Group Members

This section describes how to add and update hunt group members.

Before You Begin

Configure the pilot point for which you want to add hunt group members, including associating the directory number to the pilot point, as described in the "Configuring Pilot Points" section on page 16-21.

Procedure

Step 1 Find the pilot point for which you want to configure hunt group members as described in the "Finding a Pilot Point" section on page 16-22.

Step 2 Do one of the following:

- To add a hunt group member, click the **Add Member** button in the Hunt Group Member Information area.
- To edit an existing hunt group member, choose the hunt group member and click the **Edit Member** button in the Hunt Group Member Information area.

The Hunt Group Configuration window displays.

Step 3 Enter the appropriate configuration settings for the new hunt group member as described in Table 16-4.

Step 4 Click **Save**.

Step 5 Do one of the following

- To add a new hunt group member to the pilot point, click **Add New** and repeat Step 3 and Step 4.
- To create another hunt group member by copying the hunt group member that is displayed in the Hunt Group Configuration window, click **Copy** and repeat Step 3 and Step 4.
- To delete the hunt group member that is displayed, click **Delete**.
- To close the Hunt Group Configuration window and return to the Pilot Point Configuration window, click **Close**.

Step 6 To reorder the hunt group list, choose the member that you want to reorder from the list. Click the up and down arrows to move that member to a new position in the list.

If you are configuring a linked hunt group, make sure that the final member of each hunt group is the pilot point for the next hunt group.

Caution Cisco strongly recommends that you do not link the last hunt group back to the first hunt group.

For an example of a linked hunt group, see the "Understanding Linked Hunt Groups" section on page 16-5.

Additional Information

See the "Related Topics" section on page 16-39.

Hunt Group Configuration Settings

Table 16-4 describes hunt group configuration settings.

Table 16-4 Hunt Group Configuration Settings

Field	Description
Pilot Point	Displays the name of the pilot point for which you are configuring hunt group members.
Pilot Number (DirN)	Displays the directory number that is associated with the pilot point for which you are configuring hunt group members.
Hunt Group Member	This read-only field reflects the information that you choose from the Hunt Group Configuration window whether you enter the device directory number or the attendant console user name and line number; for example: • Call directory number 35201 (directory number example) • Direct Call to Mary Brown, Line 1 (user and line number example)
Member Option	Choose Device Member or User Member. If you choose the Device Member radio button, complete the fields in the **Device Member Information** section. If you choose the User Member, complete the User Name and Line Number fields in the **User Member Information** section. **Note** If you specify an attendant console user and line number, Cisco CallManager Attendant Console first checks whether the attendant console user is logged in to an attendant console and online before attempting to route the call. When you specify a user and line number, the user can log in to and receive calls on any Cisco IP Phone in the cluster that the attendant console controls.
Directory Number	Choose the directory number that you want to include in the hunt group. This field is only available if you chose the Device Member radio button from the Member Option field. **Caution** If you are configuring a linked hunt group, Cisco strongly recommends that you do not include any pilot point numbers in the hunt group except as the final member. Including other pilot point numbers in the hunt group may cause a continuous route loop.

Table 16-4 Hunt Group Configuration Settings (continued)

Field	Description
Always Route Member	If you want Cisco CallManager Attendant Console to always route calls to this hunt group member, whether it is busy or not, check this check box. If this check box is checked, Cisco CallManager Attendant Console does not check whether the line is available before routing the call. To manage overflow conditions, check this check box for voice-messaging or auto-attendant numbers that handle multiple, simultaneous calls. For linked hunt groups, only check the **Always Route Member** check box when you are configuring the final member of each hunt group.
User Name	From the drop-down list, choose the attendant console user that will serve as a hunt group member. This field is only available if you chose the User Member radio button from the Member Option field. Only attendant console users that are added in the Cisco CallManager Attendant Console User Configuration window appear in this list.
Line Number	From the drop-down list, choose the appropriate line numbers for the hunt group. This field is only available if you chose the User Member radio button from the Member Option field. **Note** You can add the same user to the same line only once within a single hunt group. For example, you cannot add Mary Brown, Line 1, more than once in the hunt group.

Additional Information

See the "Related Topics" section on page 16-39.

Deleting Hunt Group Members

This section describes how to delete hunt group members.

Procedure

Step 1 Choose **Application > Cisco CM Attendant Console > Pilot Point**.

The Pilot Point Configuration window displays.

Step 2 In the Hunt Group member Information group box, click the name of the member that you want to delete and click **Delete Member**.

The delete confirmation dialog box displays.

Step 3 To remove the hunt group member, click **OK**. To cancel the deletion, click **Cancel**.

Additional Information

See the "Related Topics" section on page 16-39.

Cisco CallManager Attendant Console Server Configuration

From the Service Parameters Configuration window, you can set service parameters for the Cisco CallManager Attendant Console Server service. You obtain information about the parameters by clicking the "i" button help icon in the upper, right corner of the window.

Caution Do not change any service parameters without permission of a Cisco Technical Assistance Center engineer. Doing so may cause system failure.

Perform the following steps to update Cisco CallManager Attendant Console Server service parameters.

Procedure

Step 1 Choose **System** > **Service Parameters**.

The Service Parameter Configuration window displays.

Step 2 From the Server drop-down list box, choose a server.

Step 3 From the Service drop-down list box, choose the Cisco CallManager Attendant Console Server service.

Note You must activate the Cisco CallManager Attendant Console service on a server before the server displays in the Cisco CallManager Attendant Console Servers list. For more information on activating a service, refer to the *Cisco CallManager Serviceability Administration Guide*.

The window refreshes and displays all configured service parameters for the Cisco CallManager Attendant Console service.

Step 4 Update the appropriate parameter value. To set all service parameters for this instance of the service to the default values, click the **Set to Default** button.

To view a list of parameters and their descriptions, click the **i** button in the upper, right corner of the window. To view the list with a particular parameter at the top, click that parameter in the Cisco CallManager Attendant Console Server Configuration window.

Step 5 Click **Update**.

The window refreshes, and Cisco CallManager updates the service parameter with your changes.

Additional Information

See the "Related Topics" section on page 16-39.

Creating and Uploading the CorporateDirectory.txt File

You can create and upload a CorporateDirectory.txt file if your centralized user list is located on a directory server that is separate from the Cisco CallManager server. To do this, perform the following procedure:

Procedure

Step 1 On your PC, create a corporate directory file named CorporateDirectory.txt that contains comma separated entries for each user in the format Last Name, First Name, Telephone Number, Department. Create one line for each user in the directory. You can include empty values for fields. The system ignores blank lines and lines starting with pound (#) or semi-colons (;). The following represents a sample directory file:

```
Doe, Jane, 67890, Engineering
Doe, John, 12345, Sales
Doe, Rodney, 12346, Marketing
Doe, Brian, 12347, Customer Support
Smith,,,Marketing
Clark,,,
```

Note The CorporateDirectory.txt filename is case-sensitive.

Step 2 In Cisco CallManager Administration, choose **Application > Cisco CM Attendant Console > Cisco CM Attendant Console User File Upload**.

The Attendant Console User File Upload window displays.

Tip To view a sample directory file, choose the **View Sample CorporateDirectory.txt File** link. Then, click the browser Back button to return to the Attendant Console User File Upload window. If you have previously uploaded a corporate directory file, you can view that file by clicking the **View Current CorporateDirectory.txt File** link.

Step 3 Choose **Upload File**.

The Upload File window displays.

Step 4 Browse to the CorporateDirectory.txt file and click **Upload**.

When Cisco CallManager Administration completes the file upload, a confirmation window displays.

Note Although Cisco CallManager can import any file that you specify, the system can only use data from files that are named CorporateDirectory.txt.

Step 5 Click **Close**.

Note To update the corporate directory list, update the CorporateDirectory.txt file and upload the file again. Cisco CallManager Administration overwrites the previous file.

Additional Information

See the "Related Topics" section on page 16-39.

Deleting the CorporateDirectory.txt File

If you want to use the user list generated by the Cisco CallManager Attendant Console service rather than a user list that you imported from a separate directory server, you must delete the CorporateDirectory.txt file that you imported. The Cisco CallManager Attendant Console service will generate a new AutoGenerated.txt file when the Cisco CallManager Attendant Console service starts and when the directory sync period expires if the Directory Sync Period service parameter does not equal zero.

To delete the CorporateDirectory.txt file, use the following procedure:

Procedure

Step 1 In Cisco CallManager Administration, choose **Application > Cisco CM Attendant Console > Cisco CM Attendant Console User File Upload**.

The Attendant Console User File Upload window displays.

Step 2 Click the **Delete** button that appears next to the CorporateDirectory.txt link.

Step 3 To delete the CorporateDirectory.txt file, click **OK**. To continue without deleting the file, click **Cancel**.

Note The Cisco CallManager Attendant Console service will generate a new AutoGenerated.txt file when the Cisco CallManager Attendant Console service starts and when the directory sync period expires if the Directory Sync Period service parameter does not equal zero.

Additional Information

See the "Related Topics" section on page 16-39.

Installing the Cisco CallManager Attendant Console Plug-in on an Attendant PC

You access the Cisco CallManager Attendant Console plug-in from the Cisco CallManager Application Plugin Installation window. This section describes how to install the attendant console on a user PC.

Before You Begin

Add the attendant console user and the phone that you want to associate with the attendant console to the Cisco CallManager database. For more information on adding users, see the "Configuring an Attendant Console User" section on page 16-19. For more information on adding phones, "Configuring Cisco IP Phones" section in the *Cisco CallManager Administration Guide*.

Make sure that you have administrative privileges on the attendant PC when installing Cisco CallManager Attendant Console.

Procedure

Step 1 From each Cisco CallManager Attendant Console PC, browse into a server that is running Cisco CallManager Administration and log in with administrative privileges.

Tip To browse into the server, enter https://<CM-server-name>/ccmadmin/showHome.do, where <CM-server-name> equals the name of the server, in the Address bar in the web browser.

Step 2 From Cisco CallManager Administration, choose **Application** > **Plugins**.

Step 3 Click the icon for the Cisco CallManager Attendant Console.

The Cisco CallManager Attendant Console installation wizard runs.

Step 4 To acknowledge the installation, click **Yes**.

Step 5 In the initial installation wizard window, click **Next**.

Step 6 You can install the attendant console to the default location or use the Browse button to specify a new location; after specifying a location, click **Next**.

Step 7 In the Ready to Install window, click **Next**.

Step 8 After the installation program finishes installing files, choose whether you want to restart the computer now or later; then, click **Finish**.

Step 9 If prompted, restart the computer.

If you installed Windows XP SP2 on the client PC, see the "Starting Cisco CallManager Attendant Console After Installing Windows XP SP2" section on page 16-34 for information on unblocking the firewall, so the attendant can use the attendant console.

Step 10 If the attendant does not have administrative privileges on the PC, grant read, write, and execute permissions on the folder where you installed Cisco CallManager Attendant Console. By default, you install the Cisco CallManager Attendant Console in C:\Program Files\Cisco\CallManager Attendant Console. For more information on setting folder permissions, refer to your operating system documentation.

Step 11 Configure or update any attendant console settings that you did not configure during the installation process. See the "Configuring Cisco CallManager Attendant Console Settings" section on page 16-35.

Tip If you change IP addresses of the Cisco CallManager servers or the device pool of the attendant phone changes after you install the attendant console plug-in, the attendants must close and open Cisco CallManager Attendant Console, so the application can download the list of servers in the Cisco CallManager group.

Additional Information

See the "Related Topics" section on page 16-39.

Starting Cisco CallManager Attendant Console After Installing Windows XP SP2

When you start Cisco CallManager Attendant Console for the first time after you install Windows XP SP2, a dialog box displays that indicates that Windows Firewall has blocked some features of the ACClient application. To create an exception in the Windows Firewall, so you can continue using Cisco CallManager Attendant Console, click **Unblock**. The operating system configures the exception automatically.

After you unblock the firewall, configure or update any attendant console settings that you did not configure during the installation process. See the "Configuring Cisco CallManager Attendant Console Settings" section on page 16-35.

Additional Information

See the "Related Topics" section on page 16-39.

Configuring Cisco CallManager Attendant Console Settings

Configure each attendant console to meet the following criteria:

- Provide the attendant console username and password.
- Connect to the correct Cisco CallManager Attendant Console server and directory number for the Cisco IP Phone that the attendant uses with the attendant console.

After you install the attendant console, you must configure the attendant console before a user can log in to the console. Use the procedure in this section to configure settings that are not specified during installation, to view current settings, or to update the attendant console configuration.

After it is configured, the attendant console operates with the specified settings until the administrator changes them.

Note If you change the IP addresses of the nodes in the cluster, you may also need to change the IP address in the Attendant Server Host Name or IP Address field in the Attendant Console Settings dialog box.

Procedure

Step 1 On the PC where the attendant console is installed, choose **Start** > **Programs** > **Cisco CallManager** > **Cisco CallManager Attendant Console** or click the Cisco CallManager Attendant Console icon on the desktop; then, click **Yes** to launch the attendant console.

Step 2 Click **Settings**.

Step 3 Enter the appropriate configuration settings, as described in Table 16-5.

Step 4 Click **Save**. You have now configured the settings for the attendant console, and the settings can now be used for call-distribution activities.

Additional Information

See the "Related Topics" section on page 16-39.

Attendant Console Configuration Settings

Table 16-5 describes Cisco CallManager Attendant Console configuration settings.

Table 16-5 Settings Dialog Box

Field/Check Box	Notes
Basic Tab (Cisco requires that you enter the information in the appropriate fields.)	
Attendant Server Host Name or IP Address	Enter the appropriate information in the field.
Directory Number of Your Phone	Confirm or enter the directory number of the Cisco IP Phone that the attendant uses with the attendant console. If you enter a directory number that appears on more than one device, the Device Selector dialog box displays when you click **Save**. Choose the device that you want to use with the attendant console from the drop-down list box and click OK.
Attendant Console Client CallBack Port	If you are using a firewall, specify the port that the firewall should use to send callback messages to the attendant console client. Valid port numbers include 0 and port numbers equal to or greater than 1023.
Advanced Tab (You can enter information in these optional fields to change the default settings.)	
Path of Local Directory File	If you want the console to access a local user list rather than a centralized user list from Cisco CallManager Administration, enter the path to the user list file on the attendant PC or network share that contains the directory information.
Directory Reload Interval (in seconds)	Enter the time (in seconds) that the Cisco CallManager Attendant Console server waits before reloading the user list that displays in the Directory window of the Cisco CallManager Attendant Console.
Call Processing Server Host Name or IP Address	Enter the call processing server host name or IP address if it differs from the attendant server that you specified on the Basic tab.
Local Host IP Address (for line state)	Enter the IP address that your client uses to receive line state updates. **Note** If the attendant PC has two Network Interface Cards (NICs), you can specify the IP address that will receive line state updates.
Enable Trace	Check the check box to ensure that you can troubleshoot issues that are associated with the attendant console.

Table 16-5 Settings Dialog Box (continued)

Field/Check Box	Notes
Enable Audible Alerts	To enable audible alerts that indicate when the attendant receives calls (incoming and broadcast), drops calls, parks calls, and places calls on hold as well as that indicate how long calls have been on hold, check the **Enable Audible Alerts** check box. The audible alerts sound once per call event. The "audio" subdirectory of the Cisco CallManager Attendant Console application contains the audible alert files. By default, the system specifies the directory location, C:\Program Files\Cisco\Call Manager Attendant Console\audio.
Show Accessibility Messages	To enable accessibility messages, so dialog boxes display information about the status of the attendant console, such as when call control goes up or down, check the **Show Accessibility Messages** check box.The screen reader that an attendant has installed on the PC can then read these messages.
Hold Call When Dial Pad is Active	If you want the attendant console to place a call on hold while the attendant uses the Dial Pad window, check this check box. **Note** If the attendant uses a screen reader, you may want to check this check box, so that the caller does not hear the screen reader detail the information on the window.

Additional Information

See the "Related Topics" section on page 16-39.

Configuring Held Icon Timers

The color of the held icons on the attendant console indicates how long a call has been on hold. The WaitTimeMedium parameter indicates the time before the held icon turns yellow. The WaitTimeLong parameter indicates the time before the held icon turns red. By default, the held icon turns yellow when a call remains on hold for 60 seconds and turns red when the call remains on hold for 120 seconds. To configure the duration after which the held icons change color, perform the following procedure.

Note Cisco recommends that you do not change the default values of the held icon timers.

Procedure

Step 1 Open the GlobalUI.properties files that are located on the attendant PC in the ..\Program Files\Cisco\CallManager Attendant Console\etc directory.

Step 2 To change the time before the held icon turns yellow, edit the WaitTimeMedium parameter.

Step 3 To change the time before the held icon turns red, edit the WaitTimeLong parameter.

Step 4 Save and close the GlobalUI.properties file.

Additional Information

See the "Related Topics" section on page 16-39.

Dependency Records

To find specific directory numbers, refer to the "Dependency Records Buttons" section in the *Cisco CallManager Administration Guide*.

Troubleshooting Cisco CallManager Attendant Console

Performance monitor counters for Cisco CallManager Attendant Console in real-time monitoring tool (RTMT) allow you to monitor the time that Cisco CallManager Attendant Console Server service has been running, the amount of time since the Cisco CallManager Attendant Console Server service was started, the number of calls that have occurred, the number of calls that have been redirected, the number of attendants that are registered, the number of pilot points, and the number of registered clients.

The CcmLineLinkState performance monitor for the attendant console provides a quick way to check whether the attendant console is functioning correctly:

- If the CcmLineLinkState counter is 11, this state indicates that Cisco CallManager Attendant Console Server service is functioning normally.
- The left-most digit of CcmLineLinkState indicates whether Cisco CallManager Attendant Console Server service is connected to and registered with the Cisco CallManager CTI. If this digit is 0, a problem may exist with the CTI or the directory.
- The right-most digit of CcmLineLinkState indicates whether Cisco CallManager Attendant Console Server service can perceive line state information through Cisco CallManager. If this digit is 0, a problem probably exists with Cisco CallManager.

Note When an attendant console user cannot log in to the attendant console and no line state information is available, view the CcmLineLinkState performance monitor to verify that all components of attendant console are functioning properly.

For more information about performance monitor counters and alarms, refer to the *Cisco CallManager Serviceability System Guide* and the *Cisco CallManager Serviceability Administration Guide*.

Additional Information

See the "Related Topics" section on page 16-39.

Related Topics

- End User Configuration, *Cisco CallManager Administration Guide*
- Dependency Records, *Cisco CallManager Administration Guide*
- Application Users and End Users, *Cisco CallManager System Guide*

Attendant Console

- Configuration Checklist for Cisco CallManager Attendant Console, page 16-16
- Introducing Cisco CallManager Attendant Console, page 16-1
- System Requirements for Cisco CallManager Attendant Console, page 16-12
- Interactions and Restrictions, page 16-13
- Understanding Call Queuing, page 16-9
- Configuring Cisco CallManager Attendant Console, page 16-15
- Troubleshooting Cisco CallManager Attendant Console, page 16-38

Attendant Console Server

- Understanding the Cisco CallManager Attendant Console Server, page 16-10
- Cisco CallManager Attendant Console Redundancy, page 16-11
- Cisco CallManager Attendant Console Server Configuration, page 16-31

Attendant Console User

- Understanding Cisco CallManager Attendant Console Users, page 16-2
- Finding an Attendant Console User, page 16-17
- Configuring an Attendant Console User, page 16-19
- Cisco CallManager Attendant Console User Configuration Settings, page 16-19
- Configuring the ac User, page 16-20

Hunt Groups

- Understanding Pilot Points and Hunt Groups, page 16-2
- Understanding Linked Hunt Groups, page 16-5
- Understanding Circular Hunt Groups, page 16-6
- Understanding Broadcast Hunting, page 16-8
- Configuring Hunt Groups, page 16-28
- Configuring Hunt Group Members, page 16-28
- Deleting Hunt Group Members, page 16-30
- Hunt Group Configuration Settings, page 16-29

Media Resources

- Media Resource Management, *Cisco CallManager System Guide*
- Music On Hold, page 6-1

- Understanding Music On Hold, page 6-1
- Music On Hold Audio Sources, page 6-8

Pilot Points

- Understanding Pilot Points and Hunt Groups, page 16-2
- Finding a Pilot Point, page 16-22
- Configuring a Pilot Point, page 16-23
- Deleting a Pilot Point, page 16-26
- Pilot Point Configuration Settings, page 16-24
- Resetting a Pilot Point, page 16-26
- Associating Devices and Pilot Points with the ac User, page 16-27

Dial Rules

- Application Dial Rules Configuration, *Cisco CallManager Administration Guide*
- Directory Lookup Dial Rules Configuration, *Cisco CallManager Administration Guide*

Directory Lists

- Understanding the Cisco CallManager Attendant Console Directory, page 16-9
- Creating and Uploading the CorporateDirectory.txt File, page 16-31
- Deleting the CorporateDirectory.txt File, page 16-33

Attendant Console Plug-in

- Installing the Cisco CallManager Attendant Console Plug-in on an Attendant PC, page 16-33
- Starting Cisco CallManager Attendant Console After Installing Windows XP SP2, page 16-34
- Configuring Cisco CallManager Attendant Console Settings, page 16-35
- Attendant Console Configuration Settings, page 16-35
- Configuring Held Icon Timers, page 16-37

Additional Documentation

- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Attendant Console User Guide*

CHAPTER 17

Call Display Restrictions

The Call Display Restrictions feature allows you to choose the information that will display for calling and/or connected lines, depending on the parties who are involved in the call. By using specific configuration settings in Cisco CallManager, you can choose to present or restrict the display information for each call.

For example, in a hotel environment, you may want to see the display information for calls that are made between a guest room and the front desk; however, for calls between guest rooms, you would not want the call information to display on either phone. The Call Display Restrictions feature enables this functionality.

This chapter provides the following information about using the Call Display Restrictions feature in Cisco CallManager:

- Introducing Call Display Restrictions, page 17-1
- System Requirements for Call Display Restrictions, page 17-3
- Scenarios for Using Call Display Restrictions, page 17-3
- Interactions, page 17-3
- Configuring Call Display Restrictions, page 17-5
- Related Topics, page 17-12

Introducing Call Display Restrictions

The Call Display Restrictions feature works within a Cisco CallManager cluster that is running Cisco CallManager 5.0. To enable Call Display Restrictions, you must configure the following parameters:

Translation Pattern Parameters

- Calling Line ID Presentation
- Connected Line ID Presentation

Phone Configuration/User Device Profile Parameter:

- Ignore Presentation Indicators (internal calls only)

The combination of these settings allows you to determine whether the display information for each call is allowed or restricted.

This section includes the following topics:

- Overview of Call Display Restrictions, page 17-2
- Enabling Call Display Restrictions, page 17-2

Overview of Call Display Restrictions

Call Display Restrictions allow you to selectively display or restrict calling and/or connected line display information. A hotel environment, which might have the following needs, frequently requires this functionality:

- For calls between a guest room and the front desk, both the room and the front desk should see the call information display of each other.
- For calls between guest rooms, the rooms should not see the call information display of each other.
- For calls between guest rooms and other hotel extensions (such as the club house), only the rooms should see the call information display.
- For external calls from the public switched telephone network (PSTN) to the front desk or guest rooms, the call information of the caller should not display if the display settings are restricted.
- For all calls to the front desk, the call information of internal calls should display.

Enabling Call Display Restrictions

The basis for the functionality of the Call Display Restrictions feature is calls being routed through different translation patterns before the calls are extended to the actual device. Users then dial the appropriate translation pattern numbers to achieve the display restrictions.

Translation Pattern Configuration

To enable Call Display Restrictions, configure translation patterns with different levels of display restrictions by choosing the appropriate option for the calling line ID presentation and the connected line ID presentation parameters.

See the "Configuring the Translation Pattern Parameters" section on page 17-6 for additional information about these parameters.

Tip You must configure partitions and calling search spaces, along with translation patterns. For more information about these configurations, refer to the Translation Pattern Configuration chapter in the *Cisco CallManager Administration Guide*.

Phone Configuration/User Device Profile Configuration

Next, enable the "Ignore Presentation Indicators (internal calls only)" parameter to ignore any presentation restriction that is received for internal calls and to ensure that the device will display the call information of the remote party.

See the "Configuring the Phone Configuration" section on page 17-7 for more information about this setting.

(For users who log in to phones that are enabled for Extension Mobility, configure this setting from the Cisco CallManager Administration User Device Profile window as well. For more information about interactions with Extension Mobility, see the "Extension Mobility" section on page 17-4.)

System Requirements for Call Display Restrictions

The following software components support Call Display Restrictions:

- Cisco CallManager 5.0

The following Cisco SIP and SCCP IP Phones, software-based devices, and desktop applications support Call Display Restrictions:

- Cisco IP Phones (Models 7902, 7905, 7910, 7911, 7912, 7920, 7940, 7941, 7960, 7961, 7970, 7971)
- H.323 clients (such as Microsoft NetMeeting devices)
- CTI ports (virtual devices that software-based applications use)
- Cisco IP Communicator

Scenarios for Using Call Display Restrictions

The following scenarios provide examples for using Call Display Restrictions:

- Front Desk calls Room-1—Both phones display the call information of each other.
- Front Desk calls Room-1, and Front Desk transfers the call to Room-2—The final connected parties, Room-1 and Room-2, cannot see the call information display of each other.
- External (PSTN) calls the Front Desk—The Front Desk honors the display settings of the external caller.
- External (PSTN) calls Room-1—Room-1 honors the presentation of the external caller; the external caller cannot see the call information display of Room-1.
- Room-1 calls Front Desk—Both phones display the call information of each other.
- Room-1 calls Room-2—Neither phone can see the call information display of the other.
- Room-1 calls Front Desk, and Front Desk transfers the call to Room-2—The final connected parties, Room-1 and Room-2, cannot see the call information display of each other.
- Room-1 calls Front Desk-1, and Front Desk-1 transfers the call to Front Desk-2—The final connected parties, Room-1 and Front Desk-2, can see the call information display of each other.
- Room-1 calls Room-2, and Room-2 transfers the call to Front Desk—Room-1 and Front Desk see the call information display of each other.
- Club House calls Room-1—Club House cannot display the call information; Room-1 can see the call information display.
- All parties in a conference call—All phones see “To Conference” for the call information display.

Interactions

The following sections describe how the Call Display Restrictions feature interacts with Cisco CallManager applications and call processing:

- Call Park, page 17-4
- Conference List, page 17-4

- Conference and Voice Mail, page 17-4
- Extension Mobility, page 17-4

Call Park

When the Call Display Restrictions feature is used with Call Park, you must configure an associated translation pattern for each individual call park number to preserve the Call Display Restrictions feature; you cannot configure a single translation pattern to cover a range of call park numbers.

Consider the following scenario as an example:

1. The system administrator creates a call park range of 77x and places it in a partition called P_ParkRange. (The phones in the guest rooms can see the P_ParkRange partition is made visible to the phones in the guest rooms by inclusion of it in the calling search space of the phones (CSS_FromRoom.))
2. The administrator configures a separate translation pattern for each call park directory number and configures the display settings to Restricted. (In the current scenario, the administrator creates translations patterns for 770, 771, 772...779.)

Note For the Call Display Restrictions feature to work correctly, the administrator must configure separate translation patterns and not a single translation pattern for a range of numbers (such as 77x or 77[0-9]).

3. Room-1 calls Room-2.
4. Room-2 answers the call, and Room-1 parks the call.
5. When Room-1 retrieves the call, Room-2 does not see Room-1's call information display.

See the "Call Park" section on page 9-1 for additional information about using the Call Park feature.

Conference List

When you use Call Display Restrictions, you restrict the display information for the list of participants in a conference. For more information about conference lists, refer to the "Phone Features" section in the Cisco IP Phones chapter in the *Cisco CallManager System Guide.*

Conference and Voice Mail

When Call Display Restrictions are used with features such as conference and voice mail, the call information display on the phones reflects that status. For example, when the conference feature is invoked, the call information display shows "To Conference." When voice mail is accessed by choosing the "Messages" button, the call information display shows "To Voicemail."

Extension Mobility

To use Call Display Restrictions with Extension Mobility, you enable the "Ignore Presentation Indicators (internal calls only)" parameter in both the Cisco CallManager Administration Phone Configuration window and the Cisco CallManager Administration User Device Profile window.

When you enable Call Display Restrictions with Extension Mobility, the presentation or restriction of the call information depends on the line profile that is associated with the user who is logged in to the device. That is, the configuration that is entered in the user device profile (associated with the user) overrides the configuration that is entered in the phone configuration (of the phone that is enabled for Extension Mobility).

Configuring Call Display Restrictions

To use Call Display Restrictions, make sure that you perform the following Cisco CallManager configurations:

- Configure partitions and calling search spaces before you add a translation pattern.
- Configure translation patterns with different levels of display restrictions.
- Check the "Ignore Presentation Restriction (internal calls only)" check box to ensure that the call information display for internal calls is always visible.
- Configure individual, associated translation patterns for each individual Call Park directory number, to work with the Call Park feature.

This section contains the following topics:

- Call Display Restrictions Configuration Checklist, page 17-5
- Configuring the Translation Pattern Parameters, page 17-6
- Configuring the Phone Configuration, page 17-7
- Sample Configurations, page 17-8

Call Display Restrictions Configuration Checklist

Table 17-1 provides a checklist to configure Call Display Restrictions.

Table 17-1 Call Display Restrictions Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure partitions for rooms, front desk, club, and the PSTN. See the "Partitions" section on page 17-8.	Configuring a Partition, *Cisco CallManager Administration Guide*
Step 2	Configure call park directory numbers or define a range of call park directory numbers. Configure translation patterns for each call park directory number for call park retrieval from rooms. See the "Call Park" section on page 17-11.	Configuring a Call Park Number, *Cisco CallManager Features and Services Guide*
Step 3	Configure a partition for call park directory numbers to make the partition available only to users who have the partition in their calling search space. See the "Partitions" section on page 17-8 and the "Call Park" section on page 17-11.	Configuring a Partition, *Cisco CallManager Administration Guide*
Step 4	Configure calling search spaces for rooms, front desk, club, the PSTN, and room park range (for Call Park). See the "Calling Search Spaces" section on page 17-8.	Calling Search Space Configuration, *Cisco CallManager Administration Guide*

Table 17-1 Call Display Restrictions Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 5	Configure the phones for the rooms, front desk, club, and the gateway for the PSTN. See the "Devices and Gateways" section on page 17-9.	Cisco IP Phone Configuration, *Cisco CallManager Administration Guide* Device Profile Configuration, *Cisco CallManager Administration Guide*
Step 6	Configure translation patterns and route patterns. See the "Translation Patterns" section on page 17-9.	Translation Pattern Configuration, *Cisco CallManager Administration Guide* Understanding Route Plans, *Cisco CallManager System Guide*

Configuring the Translation Pattern Parameters

Configure the following parameters from the Cisco CallManager Administration Translation Pattern Configuration window.

Tip For outgoing calls, the translation pattern setting at the terminating end can override the originating Cisco CallManager cluster settings.

Calling Line ID Presentation

Cisco CallManager uses calling line ID presentation as a supplementary service to allow or restrict the originating caller's phone number on a call-by-call basis. Choose one of the following options to allow or restrict the display of the calling party's phone number on the called party's phone display for this translation pattern:

- Default—This option does not change the calling line ID presentation.
- Allowed—Cisco CallManager allows the display of the calling number.
- Restricted—Cisco CallManager blocks the display of the calling number.

Note If the incoming call goes through a translation pattern or route pattern and the calling line ID presentation setting is allowed or restricted, the system modifies the calling line presentation with the translation or route pattern setting.

Connected Line ID Presentation

Cisco CallManager uses connected line ID presentation as a supplementary service to allow or restrict the called party's phone number on a per-call basis. Choose one of the following options to allow or restrict the display of the connected party's phone number on the calling party's phone display for this translation pattern:

- Default—This option does not change the connected line ID presentation.
- Allowed—This option displays the connected party's phone number.
- Restricted—Cisco CallManager blocks the display of the connected party's phone number.

Note If the incoming call goes through a translation or route pattern and the connected line ID presentation field is set to allowed or restricted, the system modifies the connected line presentation indicator with the translation or route pattern setting.

Examples

- For calls that are made from one guest room to another, configure the calling line ID presentation and the connected line ID presentation to restricted to ensure that the call information does not display.
- For calls that are made from the front desk to a guest room, configure the calling line ID presentation to allowed and the connected line ID presentation to restricted to ensure both parties can see the call information.

Tip For more information about calling party transformations and connected party transformations, refer to the Understanding Route Plans chapter in the *Cisco CallManager System Guide*.

Configuring the Phone Configuration

To complete the configuration of the Call Display Restrictions feature, check the “Ignore Presentation Indicators (internal calls only)” check box from the Cisco CallManager Administration Phone Configuration window.

For use with Extension Mobility, also configure this setting from the Cisco CallManager Administration User Device Profile window.

When you set the “Ignore Presentation Indicators (internal calls only)” field,

- Cisco CallManager always displays the remote party’s call information if the other party is internal.
- Cisco CallManager does not display the remote party’s call information if the other party is external and the display presentation is restricted.

Note Ensure the calling line ID presentation and the connected line ID presentation are configured with the “Ignore Presentation Indicators (internal calls only)” parameter for Cisco CallManager to ignore the presentation settings of internal callers. For incoming external calls, the system maintains the received presentation indicators even if the “Ignore Presentation Indicators (internal calls only)” parameter is set.

Example

- For phones that are used at the hotel front desk, check the “Ignore Presentation Indicators (internal calls only)” check box, so the front desk can always see the call information display for internal calls.

Tip For information about phone configurations, refer to the Cisco IP Phone Configuration chapter in the *Cisco CallManager Administration Guide.* For information about device profile configurations, refer to the Device Profile Configuration chapter in the *Cisco CallManager Administration Guide*.

Sample Configurations

The following information provides sample configurations to enable the Call Display Restrictions feature and includes the following topics:

- Partitions, page 17-8
- Calling Search Spaces, page 17-8
- Devices and Gateways, page 17-9
- Translation Patterns, page 17-9
- Call Park, page 17-11

Partitions

From the Cisco CallManager Administration Partition Configuration window, configure the following partitions:

- Insert a real partition P_Room
- Insert a real partition P_FrontDesk
- Insert a real partition P_Club
- Insert a real partition P_PSTN
- Insert a translation partition P_CallsFromRoomToRoom
- Insert a translation partition P_CallsFromRoomToFrontDesk
- Insert a translation partition P_CallsFromRoomToClub
- Insert a translation partition P_CallsFromRoomToPSTN
- Insert a translation partition P_CallsFromFrontDeskToRoom
- Insert a translation partition P_CallsFromFrontDeskToFrontDesk
- Insert a translation partition P_CallsFromFrontDeskToClub
- Insert a translation partition P_CallsFromFrontDeskToPSTN
- Insert a translation partition P_CallsFromPSTN
- Insert a translation partition P_CallsFromClubToRoom
- Insert a translation partition P_CallsFromClubToFrontDesk
- Insert a translation partition P_FrontDeskToParkNumber
- Insert a translation partition P_RoomToParkNumber
- Insert a translation partition P_ParkNumberRange

Calling Search Spaces

From the Cisco CallManager Administration Calling Search Space Configuration window, configure the following calling search spaces:

- Insert a calling search space CSS_Room {P_Room}
- Insert a calling search space CSS_FrontDesk {P_FrontDesk}
- Insert a calling search space CSS_Club {P_Club}

- Insert a calling search space CSS_PSTN {P_PSTN}
- Insert a calling search space CSS_FromRoom
  { P_CallsFromRoomToFrontDesk, P_CallsFromRoomToRoom, P_CallsFromRoomToClub, P_CallsFromRoomToPSTN, P_RoomToParkNumber, P_ParkNumberRange}
- Insert a calling search space CSS_FromFrontDesk
  { P_CallsFromFrontDeskToRoom, P_CallsFromFrontDeskToClub, P_CallsFromFrontDeskToPSTN, P_CallsFromFrontDeskToFrontDesk }
- Insert a calling search space CSS_FromPSTN
  { P_CallsFromPSTN}
- Insert a calling search space CSS_FromClub
  { P_CallsFromClubToRoom, P_CallsFromClubToFrontDesk}
- Insert a calling search space CSS_ RoomParkRange
  {P_ParkNumberRange }

Devices and Gateways

From the Cisco CallManager Administration Phone Configuration and from the Cisco CallManager Administration Gateway Configuration windows, configure the following phones and configure the following gateway:

- Configure phone A (Room-1) with partition P_Room and device/line calling search space CSS_FromRoom
  { P_Phones, CSS_FromRoom} : 221/Room-1
- Configure phone B (Room-2) with partition P_Room and device/line calling search space CSS_FromRoom
  { P_Phones, CSS_FromRoom} : 222/Room-2
- Configure phone C (Front Desk-1) with partition P_FrontDesk and device/line calling search space CSS_FromFrontDesk and Ignore Presentation Indicators check box enabled
  { P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set} : 100/Reception
- Configure phone D (Front Desk-2) with partition P_FrontDesk and device/line calling search space CSS_FromFrontDesk and Ignore Presentation Indicators check box enabled
  { P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set} : 200/Reception
- Configure phone E (Club) with partition P_Club and calling search space CSS_FromClub
  { P_Club, CSS_FromClub) : 300/Club
- Configure PSTN Gateway E with route pattern P_PSTN and calling search space CSS_FromPSTN
  {CSS_FromPSTN}, RoutePattern {P_PSTN}

Translation Patterns

From the Cisco CallManager Administration Translation Pattern Configuration window, configure the following translation patterns:

- Insert a translation pattern TP1 as 1XX
  Partition: P_CallsFromRoomToFrontDesk
  CSS: CSS_FrontDesk
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Allowed
  {P_CallsFromRoomToFrontDesk, CSS_FrontDesk, Calling Line/Name - Restricted, Connected Line/Name - Allowed}

- Insert a translation pattern TP2 as 2XX
Partition: P_CallsFromRoomToRoom
CSS: CSS_Room
Calling Line ID Presentation and Calling Name Presentation: Restricted
Connected Line ID Presentation and Connected Name Presentation: Restricted
{P_CallsFromRoomToRoom, CSS_Room, Calling Line/Name - Restricted, Connected Line/Name - Restricted}
- Insert a translation pattern TP3 as 3XX
Partition: P_CallsFromRoomToClub
CSS: CSS_Club
Calling Line ID Presentation and Calling Name Presentation: Restricted
Connected Line ID Presentation and Connected Name Presentation: Allowed
{P_CallsFromRoomToClub, CSS_Club, Calling Line/Name - Restricted, Connected Line/Name - Allowed}
- Insert a translation pattern TP4 as 9XXXX with called party transform mask as XXX
Partition: P_CallsFromRoomToPSTN
CSS: CSS_PSTN
Calling Line ID Presentation and Calling Name Presentation: Restricted
Connected Line ID Presentation and Connected Name Presentation: Default
{P_CallsFromRoomToPSTN, CSS_PSTN, Calling Line/Name - Restricted, Connected Line/Name - Default}
- Insert a route pattern RP5 as 9.XXXXXX with discard digits as predot
(DDI : PreDot)
Partition: P_CallsFromRoomToPSTN
CSS: CSS_PSTN
Calling Line ID Presentation and Calling Name Presentation: Restricted
Connected Line ID Presentation and Connected Name Presentation: Default
{P_CallsFromRoomToPSTN, CSS_PSTN, Calling Line/Name - Restricted, Connected Line/Name - Default}
- Insert a translation pattern TP6 as 2XX
Partition: P_CallsFromFrontDeskToRoom
CSS: CSS_Room
Calling Line ID Presentation and Calling Name Presentation: Allowed
Connected Line ID Presentation and Connected Name Presentation: Restricted
{P_CallsFromFrontDeskToRoom, CSS_Room, Calling Line/Name - Allowed, Connected Line/Name - Restricted}
- Insert a translation pattern TP7 as 1XX
Partition: P_CallsFromFrontDeskToFrontDesk
CSS: CSS_FrontDesk
Calling Line ID Presentation and Calling Name Presentation: Allowed
Connected Line ID Presentation and Connected Name Presentation: Allowed
{P_CallsFromFrontDeskToFrontDesk, CSS_FrontDesk, Calling Line/Name - Allowed, Connected Line/Name - Allowed}
- Insert a translation pattern TP8 as 3XX
Partition: P_CallsFromFrontDeskToClub
CSS: CSS_Club
Calling Line ID Presentation and Calling Name Presentation: Allowed
Connected Line ID Presentation and Connected Name Presentation: Allowed
{P_CallsFromFrontDeskToClub, CSS_Club, Calling Line/Name - Allowed, Connected Line/Name - Allowed}

- Insert a translation pattern TP9 as 9XXXX
  Partition: P_CallsFromFrontDeskToPSTN
  CSS: CSS_PSTN
  Calling Line ID Presentation and Calling Name Presentation: Allowed
  Connected Line ID Presentation and Connected Name Presentation: Default
  {P_CallsFromFrontDeskToPSTN, CSS_PSTN, Calling Line/Name - Allowed, Connected Line/Name - Default}
- Insert a route pattern RP10 as 9.XXXX with discard digits as predot
  Partition: P_CallsFromFrontDeskToPSTN
  CSS: CSS_PSTN
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Default
  {P_CallsFromFrontDeskToPSTN, CSS_PSTN, Calling Line/Name - Restricted, Connected Line/Name - Default}
- Insert a translation pattern TP11 as 1XX
  Partition: P_CallsFromClubToFrontDesk
  CSS: CSS_FrontDesk
  Calling Line ID Presentation and Calling Name Presentation: Allowed
  Connected Line ID Presentation and Connected Name Presentation: Allowed
  {P_CallsFromClubToFrontDesk, CSS_FrontDesk, Calling Line/Name - Allowed, Connected Line/Name - Allowed}
- Insert a translation pattern TP12 as 2XX
  Partition: P_CallsFromClubToRoom
  CSS: CSS_Room
  Calling Line ID Presentation and Calling Name Presentation: Allowed
  Connected Line ID Presentation and Connected Name Presentation: Restricted
  { P_CallsFromClubToRoom, CSS_Room, Calling Line/Name - Allowed, Connected Line/Name - Restricted}
- Insert a translation pattern TP13 as 1XX
  Partition: P_CallsFromPSTN
  CSS: CSS_FrontDesk
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Allowed
  { P_CallsFromPSTN, CSS_FrontDesk, Calling Line/Name - Restricted, Connected Line/Name - Allowed}

Call Park

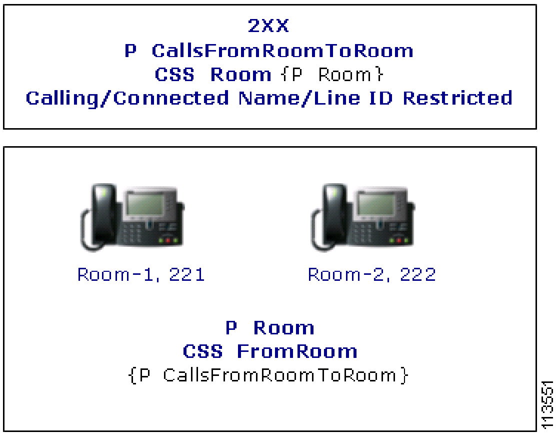
From the Cisco CallManager Administration Call Park Configuration window, configure the following items for the Call Park feature:

- Insert a Call Park directory number 888X
  Call Park Range: P_ParkNumberRange/888X
- Configure the translation patterns for the call park retrieval from
  room: TP (11-20): 8880 to 8889
  Partition: P_RoomToParkNumber
  CSS: CSS_RoomParkRange
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Restricted

Sample Call Flow

Figure 17-1 shows a graphic representation of a sample call flow, with a description of how the Call Display Restrictions feature works in this scenario.

Figure 17-1 Sample Call Flow



1. Room-1 calls Room-2 (directory number 222).
2. Room-1 has CSS_FromRoom, so Room-1 can access only phones that are in the P_CallsFromRoomToRoom partition.
3. The P_CallsFromRoomToRoom partition contains 2XX, but it does not contain directory number 222 (Room-2).
4. The call routes to translation pattern TP:2XX, which is configured to restrict display information.
5. The TP:2XX translation pattern can access the P_Room partition because it is configured with the CSS_Room calling search space.
6. The CSS_Room calling search space contains directory number 222 (Room-2).
7. The call connects to Room-2, but theTP:2XX translation pattern restricts the display information.

Related Topics

- Translation Pattern Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Calling Search Space Configuration, *Cisco CallManager Administration Guide*
- Device Profile Configuration, *Cisco CallManager Administration Guide*
- Partition Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phones, *Cisco CallManager System Guide*
- Phone Features, *Cisco CallManager System Guide*

Additional Cisco Documentation

- *Cisco CallManager Serviceability System Guide*

- *Cisco CallManager Serviceability Administration Guide*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- Cisco IP Phone user documentation and release notes (all models)

CHAPTER 18

Quality Report Tool

The Quality Report Tool (QRT), a voice-quality and general problem-reporting tool for Cisco IP Phones, acts as a service that allows users to easily and accurately report audio and other general problems with their IP phone. QRT automatically loads with the Cisco CallManager installation, and the Cisco Extended Functions (CEF) service supports it. (For more information about the Cisco Extended Functions service, refer to the *Cisco CallManager Serviceability System Guide* and the *Cisco CallManager Serviceability Administration Guide*.)

As system administrator, you can enable QRT functionality by creating, configuring, and assigning a softkey template to associate the QRT softkey on a user's IP phone. You can choose from two different user modes, depending upon the amount of user interaction with QRT that is desired.

Note The system gives users with administrator privileges the authorization to configure QRT and view the reports.

This chapter provides the following information about configuring and using the QRT feature:

- Introducing Quality Report Tool, page 18-1
- System Requirements for QRT, page 18-5
- Cisco Extended Functions Service Dependency, page 18-5
- Securing a TLS Connection to CTI, page 18-7
- How to Use QRT, page 18-8
- Interactions and Restrictions, page 18-14
- Installing and Activating QRT Functions, page 18-14
- Configuring the QRT Feature, page 18-15
- Using the QRT Viewer, page 18-26
- Providing Information to Users for the QRT Feature, page 18-31
- Troubleshooting the QRT Feature, page 18-31
- Related Topics, page 18-32

Introducing Quality Report Tool

When you install Cisco CallManager, the Cisco Extended Functions service installs and loads the QRT functionality on the Cisco CallManager server.

Then, as system administrator, you enable the QRT feature through the use of softkey templates and define how the feature will work in your system by configuring system parameters and setting up Cisco CallManager Serviceability tools. You can then create, customize, and view phone problem reports by using the QRT Viewer application. (The system includes the QRT Viewer application as part of the Cisco CallManager Serviceability Real-Time Monitoring Tool. See the "Using the QRT Viewer" section on page 18-26 for more information.)

You can configure QRT availability for up to four different call states and choose from two different user modes. The user modes determine the level of user interaction that is enabled with QRT and allow either detailed voice-quality reports or more general phone problem reports and relevant statistics. (See the "Extended Menu Choices" section on page 18-9 for more information.)

When users experience problems with their IP phones, they can invoke this feature by pressing the QRT softkey on their Cisco IP Phone during one of the following call states:

- Connected
- Connected Conference
- Connected Transfer
- On Hook

From a supported call state, and using the appropriate problem classification category, users can then choose the reason code that best describes the problem that they are experiencing with their IP phone. See the "Problem Classification Categories and Reason Codes" section on page 18-10 for specific information about problem categories, reason codes, and supported call states.

The Quality Report Tool comprises several key components. The following sections provide information about these components and the architecture of the QRT feature:

- Components of QRT, page 18-2
- Overview of QRT Architecture, page 18-3

Additional Information

See the "Related Topics" section on page 18-32.

Components of QRT

QRT, a multitiered, web-based application, includes the following key components:

- Client Components
  - IP phone browser for end-user interface
  - Cisco CallManager Administration windows for feature and tools configuration and viewer application
- Server Components
  - Cisco Extended Functions service
  - Cisco CallManager for skinny messages
  - CTIManager for QBE messages
  - Database for configuration data and device data
  - Cisco RIS Data Collector for runtime device-related information
  - Alarm interface
  - System Diagnostic Interface (SDI) trace

- Service—Cisco Extended Functions service for collecting and managing user reports. It also handles the user interface on the IP phone as well as notifying Cisco RIS Data Collector for alerts and issuing SNMP traps.
- Viewer Application—The QRT Viewer application, which is included as part of the trace collection feature in the Cisco Real-Time Monitoring Tool (RTMT), allows you to filter, format, and view generated reports. Reports automatically open in the QRT Viewer when you view a trace file that includes QRT information.

Additional Information

See the "Related Topics" section on page 18-32.

Overview of QRT Architecture

The QRT feature uses the Cisco Extended Functions service, which comprises the following interfaces:

- Cisco CTIManager Interface (QBEHelper), page 18-4
- Cisco CallManager Database Interface (DBL Library), page 18-4
- Screen Helper and Dictionary, page 18-4
- Redundancy Manager, page 18-4
- DB Change Notifier, page 18-5
- SDI Trace and Alarm, page 18-5

The Cisco Extended Functions service interfaces with the phone by using the XML services interface (XSI) over skinny protocol (a protocol that is used between a Cisco IP Phone and Cisco CallManager) and the Quick Byte Encoding protocol (a protocol that is used between the Cisco CTIManager and TSP/JTAPI).

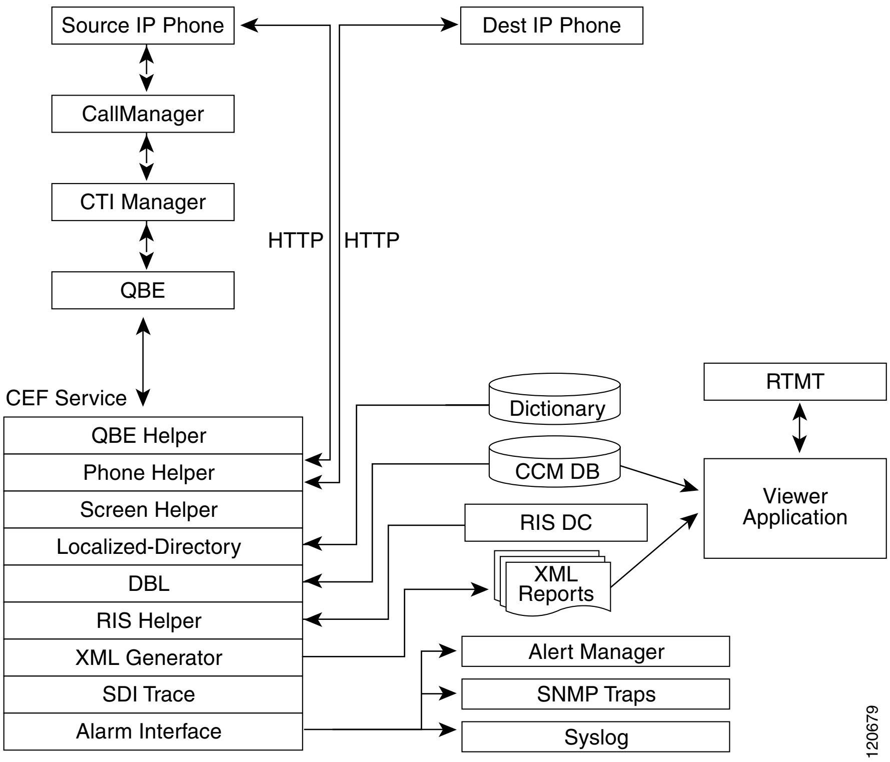
When a user presses the QRT softkey, QRT opens the device and presents up to four different screens that display problem categories and associated reason codes to obtain user feedback.

After the user chooses the option that best describes the problem, the system logs the feedback in the XML file; the system then issues alarms to notify the Cisco RIS Data Collector to generate alerts and SNMP traps. When QRT detects that user interaction is complete, it then closes the device.

Note The actual information that is logged depends upon the user selection and whether the destination device is a Cisco IP Phone.

Figure 18-1 shows an illustration of the Cisco Extended Functions service architecture.

Figure 18-1 Using the Cisco Extended Functions Service Architecture



Cisco CTIManager Interface (QBEHelper)

The QBEHelper library provides the interface that allows the Cisco Extended Functions service to communicate with a configured Cisco CTIManager.

Cisco CallManager Database Interface (DBL Library)

The DBL library provides the interface that allows the Cisco Extended Functions service to perform queries on various devices that are configured and registered in the Cisco CallManager database.

Screen Helper and Dictionary

The screen helper of the Cisco Extended Functions service reads the XML dictionary files and creates Document Object Model (DOM) objects for all installed locales when the CEF service starts. The system uses these DOM objects for constructing XSI screens that the Cisco IP Phone needs.

Redundancy Manager

When multiple Cisco Extended Functions are active within a Cisco CallManager cluster, the redundancy manager uses an algorithm to determine which CEF service is active and which is the backup CEF. The Redundancy Manager uses the lowest IP address of the server that is running the CEF service as the active service. The remaining CEF services serve as backup services.

DB Change Notifier

The DB Change Notifier handles all the database change notifications, such as service parameter changes, trace parameter changes, alarm configuration changes, and status changes of other Cisco Extended Functions services in the cluster, and reports the changes to the CEF service.

SDI Trace and Alarm

The Cisco Extended Functions service uses the SDI Trace and Alarm libraries. The libraries generate traces and alarms to the Event Viewer. The alarm library publishes information about the CEF service to Syslog, SNMP, and the Cisco RIS Data Collector service. For more information about traces and alarms, refer to the *Cisco CallManager Serviceability Administration Guide*.

Additional Information

See the "Related Topics" section on page 18-32.

System Requirements for QRT

To operate, the QRT feature requires the following software components:

- Cisco CallManager 3.3 or later
- Microsoft Windows 2000 or non-Windows-based OS (client application)
- Microsoft Internet Explorer or Netscape Navigator

Support for the QRT feature extends to any model IP phone that includes the following capabilities:

- Support for softkey templates
- Support for IP phone services
- Controllable by CTI
- An internal HTTP server

Note For more information, refer to the following URL for the appropriate Cisco IP Phone guide for your model IP phone: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm.

Additional Information

See the "Related Topics" section on page 18-32.

Cisco Extended Functions Service Dependency

The Cisco Extended Functions service depends on the following services:

- Cisco CallManager—Ensure a minimum of one Cisco CallManager service is running in the cluster, but the service need not be on the same server as CEF.
- Cisco CTIManager—Ensure a minimum of one Cisco CTIManager service is running in the cluster, but the service need not be on the same server as CEF.

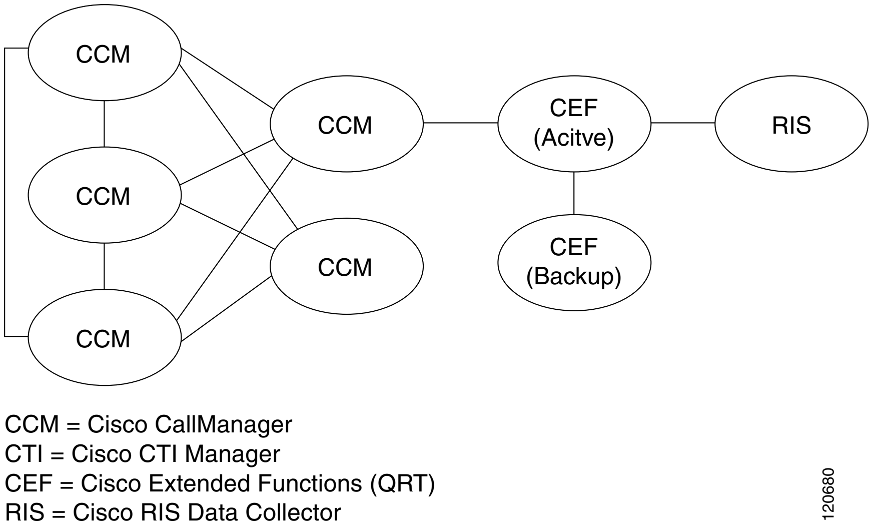
- Cisco Database Layer Monitor—Ensure one Cisco Database Layer Monitor service is running on the same server as CEF.
- Cisco RIS Data Collector—Ensure one Cisco RIS Data Collector service is running on the same server as CEF.

Note Ensure Cisco Database Layer Monitor and Cisco RIS Data Collector are running on the same server. You can include more than one CEF service in a Cisco CallManager cluster.

Tip Install all the services on one server for one-server Cisco CallManager systems.

Figure 18-2 shows a typical Cisco Extended Functions service configuration.

Figure 18-2 Cisco Extended Functions Service Dependency (Typical Configuration)



Additional Information

See the "Related Topics" section on page 18-32.

Multiple Cisco Extended Functions Applications in a Cluster

If multiple Cisco Extended Functions services are active within a Cisco CallManager cluster, CEF uses an algorithm to determine which service should be active and to order the remaining as backups. The CEF application with the lowest IP address becomes active. The service with the next lowest IP address becomes the backup to the active service. Any remaining services act as backups to each other, beginning with the service with the next lowest IP address. If you add any new services to the cluster, CEF restarts the algorithm to determine which service will be active.

Note When a Cisco Extended Functions service gets started in a cluster, the CEF service with the lowest IP address becomes active. This process may cause service interruption for approximately 2 minutes.

To verify the directory status and Cisco Extended Functions service registration status to the Cisco CTIManager, use the Real-Time Monitoring Tool (RTMT) as described in the *Cisco CallManager Serviceability Administration Guide*.

Additional Information

See the "Related Topics" section on page 18-32.

Securing a TLS Connection to CTI

QRT supports a secure Transport Layer Security (TLS) connection to CTI. Obtain the secure connection by using the "CCMQRTSecureSysUser" application user, as described in the following procedure.

Note If you enable security from the service parameters window, the QRT will open a secure connection to CTI Manager by using the Application CAPF profile. You should configure both the "CTI Manager Connection Security Flag" and the "CAPF Profile Instance Id for Secure Connection to CTI Manager" service parameters for the secure connection to succeed. See the "Setting the Cisco Extended Functions Service Parameters for QRT" section on page 18-24. For more information, refer to "Application User CAPF Profile Configuration" and "Service Parameters Configuration" in the *Cisco CallManager Administration Guide*.

Note You must also configure the security service parameter "Cluster Security Mode CAPF Phone Port" to secure a TLS connection to CTI, giving it a value of 1. You can do this from **System > Enterprise Parameters** in Cisco CallManager Administration. Refer to "Enterprise Parameters Configuration" in the *Cisco CallManager Administration Guide*.

Perform the following procedure to configure the application user.

Procedure

Step 1 From Cisco CallManager Administration, choose **User Management > Application User.**

The Find and List Application Users window displays.

Step 2 Click **Find**.

Step 3 From the Application User Configuration window, click **CCMQRTSecureSysUser** or **CCMQRTSysUser**.

Note To configure a CAPF profile, refer to "Application User CAPF Profile Configuration" in the *Cisco CallManager Administration Guide*.

Additional Information

See the "Related Topics" section on page 18-32.

How to Use QRT

After you properly install and configure QRT, the QRT softkey can be configured on certain Cisco IP Phone models. See the "System Requirements for QRT" section on page 18-5 for the IP phone models that are supported with QRT.

Note The Cisco CallManager Standard User template does not include the QRT softkey. You must enable QRT functionality and make it available to users through the use of a QRT softkey. To do this, create, configure, and assign the QRT softkey from Cisco CallManager Administration. See the "Configuring the QRT Feature" section on page 18-15 for information about setting up the softkey template.

The following sections describe the user interaction features with QRT:

- User Interface, page 18-8
- Extended Menu Choices, page 18-9
- Problem Classification Categories and Reason Codes, page 18-10

For more user-related information, refer to the following URL for the appropriate Cisco IP Phone guide for your phone model:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm.

Additional Information

See the "Related Topics" section on page 18-32.

User Interface

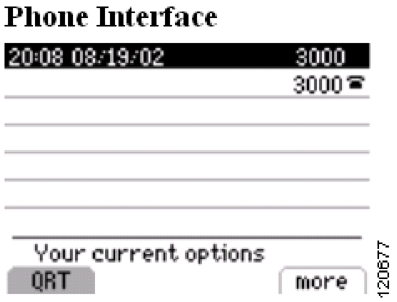
The QRT user interface includes several components:

- Phone Screens—Available to all IP phones that are in the device pool where the QRT softkey is configured, the phone screen supports different locales.

  Only the Cisco CallManager administrator can access the following components:
- Serviceability—See the "Configuring the Cisco CallManager Serviceability Features" section on page 18-21.
- Alert Configuration—See the "Configuring Alarms and Traces for QRT" section on page 18-23.
- Service Parameters—See the "Setting the Cisco Extended Functions Service Parameters for QRT" section on page 18-24.
- Viewer Application—See the "Using the QRT Viewer" section on page 18-26.

Figure 18-3 shows an example of the QRT softkey as it displays on a Cisco IP Phone.

Figure 18-3 QRT Phone Interface Display



Phone Interface

20:08 08/19/02 3000

3000

Your current options

Additional Information

See the "Related Topics" section on page 18-32.

Extended Menu Choices

Extended menu choices allow a user to interact with QRT and provide additional details regarding the phone problem that they are reporting. You can choose to enable extended menu choices or provide users with a more passive interface, depending upon the amount of information that you want users to submit.

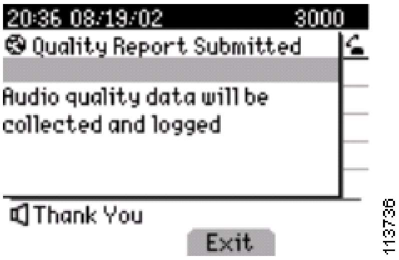
From the Cisco CallManager Service Parameters Configuration window, configure the user interface mode for QRT from the following options:

- Silent Mode—In this mode, the user does not get presented with extended menu choices. When the user presses the QRT softkey, the system collects the streaming statistics and logs the report without additional user interaction.

  The system supports silent mode only when the IP phone is in the Connected, Connected Conference, or Connected Transfer call state.

  Figure 18-4 shows an example of the QRT display as it appears in silent mode.

Figure 18-4 Submitting Voice Quality Feedback in Silent Mode



20:36 08/19/02 3000

Quality Report Submitted

Audio quality data will be collected and logged

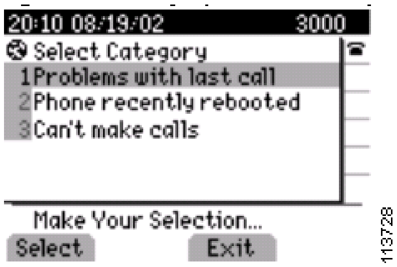
Thank You

- Interview Mode—In this mode, the user gets presented with extended menu choices, which allow additional user input that is related to audio quality on the IP phone (see the "Problem Classification Categories and Reason Codes" section on page 18-10 for the applicable reason codes). This mode also allows the user to report other, non-audio-related problems such as the phone rebooting or the inability to make calls.

  The system supports interview mode only when the IP phone is in the Connected or On Hook call state.

Figure 18-5 shows an example of the QRT display as it appears when the QRT softkey is pressed while the phone is on hook and in interview mode.

Figure 18-5 QRT Phone Interface - On Hook, Interview Mode Display



20:10 08/19/02 3000

Select Category

1 Problems with last call

2 Phone recently rebooted

3 Can't make calls

Make Your Selection...

Note Ensure that you configure the QRT softkey only for the supported call states.

Note Configure the “Display extended menu choices” field in the Cisco CallManager Administration Service Parameters configuration window to determine whether the users can access the extended menu choices. See the “Setting the Cisco Extended Functions Service Parameters for QRT” section on page 18-24 for additional information.

Additional Information

See the “Related Topics” section on page 18-32.

Problem Classification Categories and Reason Codes

The following tables show the problem categories and corresponding reason codes that users can choose when they report problems with their IP phones.

- Additional options become available after you configure extended menu choices.
- Users can choose only one reason code per category, per problem.
- Each problem category becomes available only when the IP phone is in the supported call state.

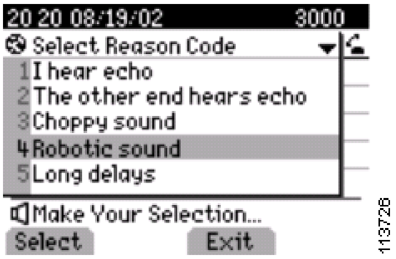
Table 18-1 shows the supported call states and the reason codes that are available for the “Problems with current call” category.

Table 18-1 Problem Category—Problems with Current Call

Problem Category	Supported Call States	Reason Codes	Statistics
Problems with current call	• Connected • Connected Conference • Connected Transfer	• I hear echo • The remote end hears echo • Choppy audio • Robotic sound • Long delays • Low volume • The remote end experiences low volume • I can't hear the remote end • The remote end can't hear me	The system collects streaming statistics from the source and destination devices. **Note** Source device/IP phone refers to the device on which the QRT softkey gets pressed. For example, "source" and "destination" in this case do not refer to the calling party and called party in a connected call.

Figure 18-6 shows an example of the phone display as it appears after the QRT softkey is pressed on an IP phone in the connected state. This menu allows the user to provide additional details before submitting a problem with the current phone call.

Figure 18-6 Reporting Problem with the Current Call



20 20 08:19:02 3000

Select Reason Code

1 I hear echo
2 The other end hears echo
3 Choppy sound
4 Robotic sound
5 Long delays

Make Your Selection...

Select Exit

Table 18-2 shows the supported call state and the reason codes that are available for the "Problems with last call" category.

Table 18-2 Problem Category—Problems with Last Call

Problem Category	Supported Call States	Reason Codes	Statistics
Problems with last call	• On Hook	• I heard echo • The remote end heard echo • Choppy audio • Robotic sound • Long delays • Low volume on my end • Low volume on the remote end • I could not hear the remote end • The remote end could not hear me • The call dropped	The system collects streaming statistics from the source device.

Figure 18-7 shows an example of the phone display as it appears after the user selects the "Problems with last call" category. This menu allows the user to provide additional details before submitting a problem report for the last phone call.

Figure 18-7 Reporting Problem with the Last Call

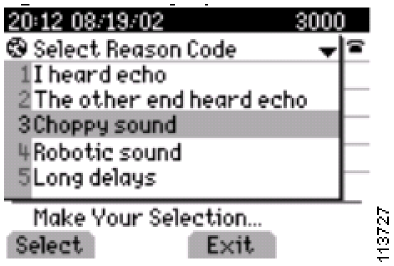


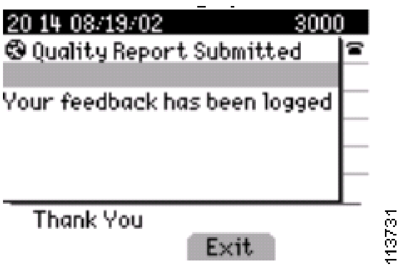
Table 18-3 shows the supported call state that is available for the "Phone recently rebooted" category. No associated reason codes exist for this category.

Table 18-3 Problem Category—Phone Recently Rebooted

Problem Category	Supported Call States	Reason Codes	Statistics
Phone recently rebooted	• On Hook	None	

Figure 18-8 shows an example of the phone display after the user chooses the "Phone recently rebooted" category. The system logs user feedback.

Figure 18-8 Reporting Problem with Phone That Recently Rebooted



20 14 08/19/02 3000

Quality Report Submitted

Your feedback has been logged

Thank You

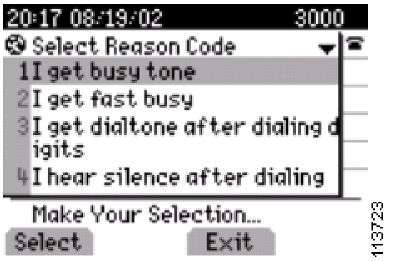
Table 18-4 shows the supported call state and the reason codes that are available for the “I can’t make calls” category.

Table 18-4 Problem Category—I Can’t Make Calls

Problem Category	Supported Call States	Reason Codes	Statistics
I can’t make calls	• On Hook	• I get a busy tone • I get a fast busy tone • I get dialtone after dialing digits • I hear silence after dialing • I don’t get dialtone	

Figure 18-9 shows an example of the phone display as it appears after the user chooses the “I can’t make calls” category.

Figure 18-9 Reporting Problem with I Can’t Make Calls



20:17 08/19/02 3000

Select Reason Code

1 I get busy tone
2 I get fast busy
3 I get dialtone after dialing digits
4 I hear silence after dialing

Make Your Selection...

Note QRT collects information from various sources, such as the source IP phone, the destination IP phone, the Cisco RIS Data Collector, the Cisco CallManager database, and the user. “Source” and “destination” in this case do not refer to the calling party and called party in a connected call. See the “QRT Reports” section on page 18-26 for detailed information about the fields that the phone problem report includes.

Additional Information

See the “Related Topics” section on page 18-32.

Interactions and Restrictions

The following interactions and restrictions apply when you use the QRT feature with Cisco CallManager:

- Ensure that Cisco Extended Functions, Cisco CallManager, CTI Manager, and Cisco RIS Data Collector services are running and fully operational.
- As system administrator, you must create, configure, and assign softkey templates to enable the QRT softkey feature on IP phones.
- Ensure that you configure the QRT softkey only for the supported call states.
- The system makes the extended menu choices option available only when the "Display extended menu choices" service parameter is set to True; it provides support for the "Problems with current call" category.
- If another application feature (such as Cisco Call Back or IPMA) or a function key (such as Settings, Directories, or Messages) is invoked while the user is interacting with QRT, or if the user does not complete the QRT selection, the system can overwrite the QRT display. In this case, the system forces the device into a wait state, which prevents QRT from completing the interaction and then closes the device.

Note Because unattended devices consume large amounts of resources and could impact CTI performance, the system configures QRT to regularly check for opened devices. You cannot modify these system settings.

- SIP phone that is configured to use UDP as the transport, instead of TCP, will not support the "device data pass-through" functionality. QRT requires the pass-through functionality, so QRT does not support these UDP-configured SIP phones.

Additional Information

See the "Related Topics" section on page 18-32.

Installing and Activating QRT Functions

As a feature within the Cisco Extended Functions service, QRT automatically installs as part of the Cisco CallManager installation.

Perform the following steps after installation to enable QRT availability for users and to set up administrative reporting capabilities:

1. Properly configure the QRT feature for Cisco IP Phone users. See the "Configuring the QRT Feature" section on page 18-15.
2. From Cisco CallManager Serviceability, activate the Cisco Extended Functions service and configure alarms and traces for use with QRT. See the "Configuring the Cisco CallManager Serviceability Features" section on page 18-21 and refer to the *Cisco CallManager Serviceability Administration Guide* for additional information.
3. Define how the QRT feature will work in your system by configuring the applicable service parameters for the Cisco Extended Functions service. See the "Setting the Cisco Extended Functions Service Parameters for QRT" section on page 18-24.

4. Create, customize, and view phone problem reports by using the QRT Viewer application. See the "Using the QRT Viewer" section on page 18-26.

Note If users require the QRT feature to display (softkeys and messages on the IP phone) in any language other than English, verify that the locale installer is installed before configuring QRT. Refer to the Cisco IP Telephony Locale Installer documentation for more information.

Additional Information

See the "Related Topics" section on page 18-32.

Configuring the QRT Feature

For successful configuration of the QRT feature, review the steps in Table 18-5, QRT Configuration Checklist, perform the configuration requirements, activate the Cisco Extended Functions service, and set the service parameters.

The following sections provide configuration information for enabling QRT:

- Configuration Checklist for QRT, page 18-16
- Creating a Softkey Template with the QRT Softkey, page 18-16
- Configuring the QRT Softkey Template in Device Pool, page 18-19
- Adding the QRT Softkey Template in Phone Configuration, page 18-20
- Activating the Cisco Extended Functions Service for QRT, page 18-22
- Configuring Alarms and Traces for QRT, page 18-23
- Setting the Cisco Extended Functions Service Parameters for QRT, page 18-24
- Related Topics, page 18-32

Configuration Checklist for QRT

Table 18-5 shows the steps for configuring the QRT feature in Cisco CallManager. For additional information, see the "Related Topics" section on page 18-32.

Table 18-5 QRT Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Create a copy of the Standard User softkey template and add the QRT softkey for the following call states: • On Hook • Connected • Connected Conference • Connected Transfer	Creating a Softkey Template with the QRT Softkey, page 18-16 Softkey Template Configuration, *Cisco CallManager Administration Guide*
Step 2	Add the new softkey template to the device pool.	Configuring the QRT Softkey Template in Device Pool, page 18-19 Device Pool Configuration, *Cisco CallManager Administration Guide*
Step 3	Add the new softkey template to the user phones by using the Phone Configuration window. **Note** You can assign the device pool to the phone configuration if you are using device pool for the softkey. Alternatively, you can add the softkey individually to each phone.	Adding the QRT Softkey Template in Phone Configuration, page 18-20 Softkey Template Configuration, *Cisco CallManager Administration Guide*
Step 4	Using the Cisco CallManager Serviceability tool, Service Activation, activate Cisco Extended Functions service.	Activating the Cisco Extended Functions Service for QRT, page 18-22 *Cisco CallManager Serviceability Administration Guide*
Step 5	From Cisco CallManager Serviceability, configure alarms and traces for QRT.	Configuring Alarms and Traces for QRT, page 18-23 *Cisco CallManager Serviceability Administration Guide*
Step 6	Configure the Cisco Extended Functions service parameters for QRT.	Setting the Cisco Extended Functions Service Parameters for QRT, page 18-24
Step 7	Access the QRT Viewer to create, customize, and view IP phone problem reports.	Using the QRT Viewer, page 18-26 *Cisco CallManager Serviceability Administration Guide.*

Creating a Softkey Template with the QRT Softkey

Perform the following procedure to create a new softkey template with the QRT softkey.

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Device Settings > Softkey Template**.

Step 2 Click **Add New**. (Alternatively, you can click the **Find** button to view a list of the available softkey templates.)

a. If you click the **Add New** button, choose the Standard User softkey template from the Softkey Template drop-down list.

b. If you click the **Find** button to view a list of the available softkey templates, choose the Standard User softkey template from the Softkey Template list.

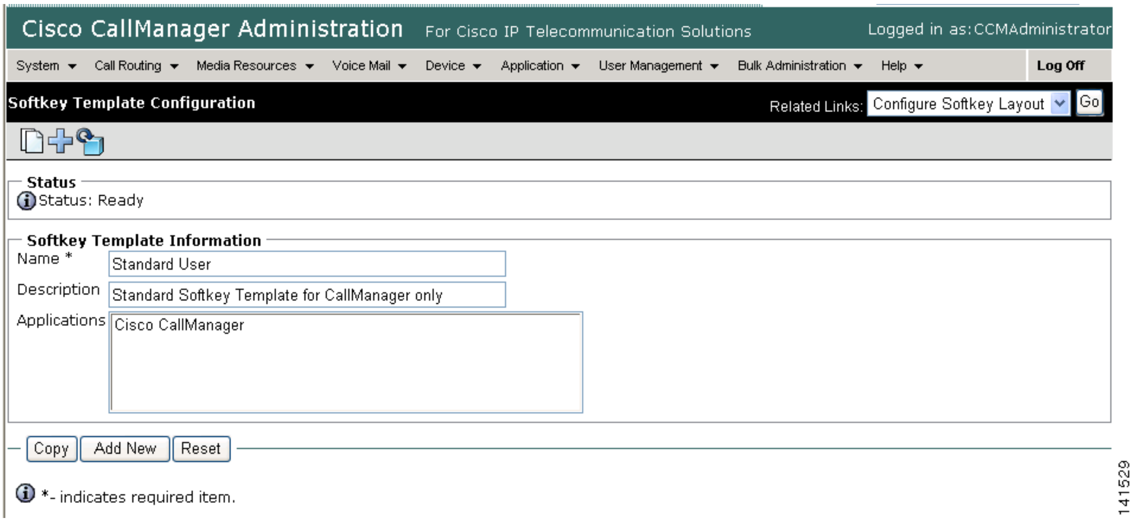
Step 3 Click the **Copy** button.

The Softkey Template Configuration window displays with new information.

Step 4 In the Softkey Template Name field, enter a new name for the template; for example, QRT Standard User; then, add a description.

Figure 18-10 shows an example of the Cisco CallManager Administration Softkey Template window where you copy a softkey template.

Figure 18-10 Softkey Template Configuration Window



Softkey Template Configuration

Status

Status: Ready

Softkey Template Information

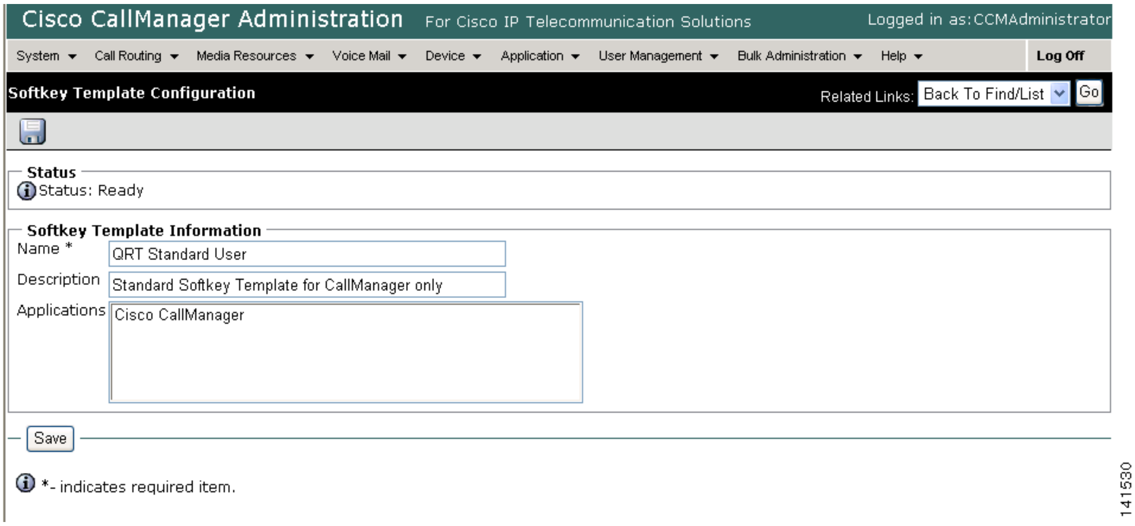
Name * Standard User

Description Standard Softkey Template for CallManager only

Applications Cisco CallManager

*- indicates required item.

Figure 18-11 Softkey Template Configuration Window After Copy



Status
Status: Ready

Softkey Template Information

Name * QRT Standard User

Description Standard Softkey Template for CallManager only

Applications Cisco CallManager

*- indicates required item.

Step 5 Click **Save**.

The Softkey Template Configuration redisplays with new information.

Step 6 To add an application, click the **Add Application** button. Refer to the "Adding Application Softkeys to Nonstandard Softkey Templates" section of the *Cisco CallManager Administration Guide* for detailed instructions.

Step 7 To add the QRT softkey to the template, choose **Configure Softkey Layout** from the Related Links drop-down list box on the Softkey Template Configuration window and click **Go**.

The Softkey Layout Configuration window displays.

Note You must add the QRT softkey to the Connected, Connected Conference, Connected Transfer, and On Hook call states.

Step 8 To add the QRT softkey to the On Hook call state, choose **On Hook** from the call states drop-down list box.

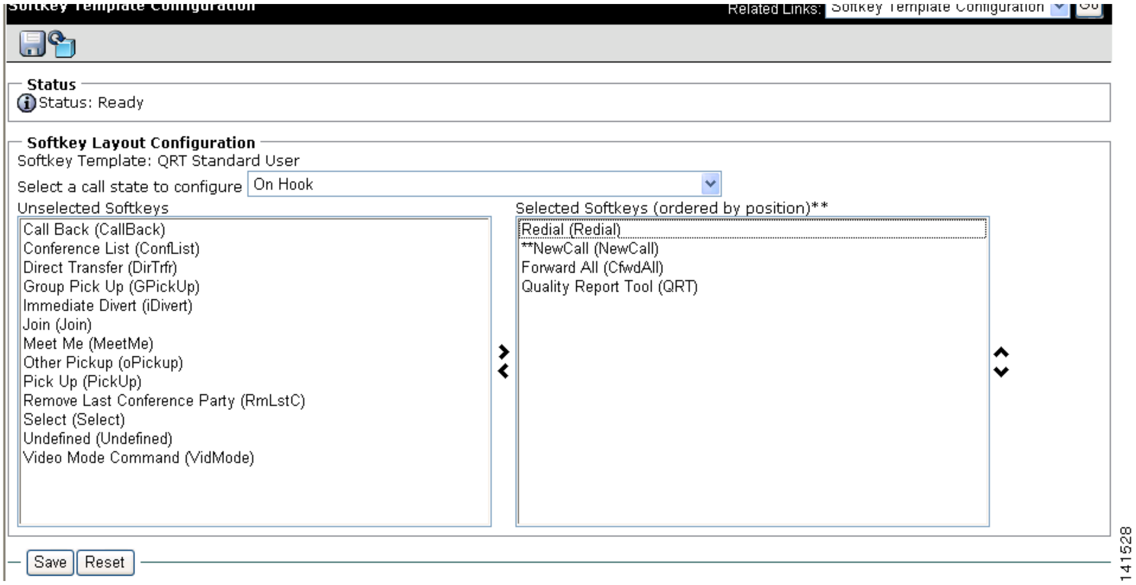
The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 9 From the Unselected Softkeys list, choose the **Quality Report Tool (QRT)** softkey and click the right arrow to move the softkey to the Selected Softkeys list.

You can prioritize the items in the Selected Softkeys list by using the up and down arrow keys.

Figure 18-12 shows an example of the Cisco CallManager Administration Softkey Layout Configuration window.

Figure 18-12 QRT Softkey Layout Configuration



Softkey Template Configuration   Related Links: Softkey Template Configuration

Status
Status: Ready

Softkey Layout Configuration
Softkey Template: QRT Standard User
Select a call state to configure: On Hook

Unselected Softkeys
- Call Back (CallBack)
- Conference List (ConfList)
- Direct Transfer (DirTrfr)
- Group Pick Up (GPickUp)
- Immediate Divert (iDivert)
- Join (Join)
- Meet Me (MeetMe)
- Other Pickup (oPickup)
- Pick Up (PickUp)
- 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)
- Quality Report Tool (QRT)

Step 10 To save and continue, click **Save**.

Step 11 To add the QRT softkey to the Connected, Connected Conference, and Connected Transfer call states, repeat Step 8 through Step 10 for each individual call state.

Note Ensure that you configure the QRT softkey only for the supported call states and click the **Save** button after each entry.

Additional Information

See the "Related Topics" section on page 18-32.

Configuring the QRT Softkey Template in Device Pool

Perform the following procedure to add the QRT softkey template to the device pool.

Procedure

Step 1 From Cisco CallManager Administration, choose **System > Device Pool**.

Step 2 Click **Find**.

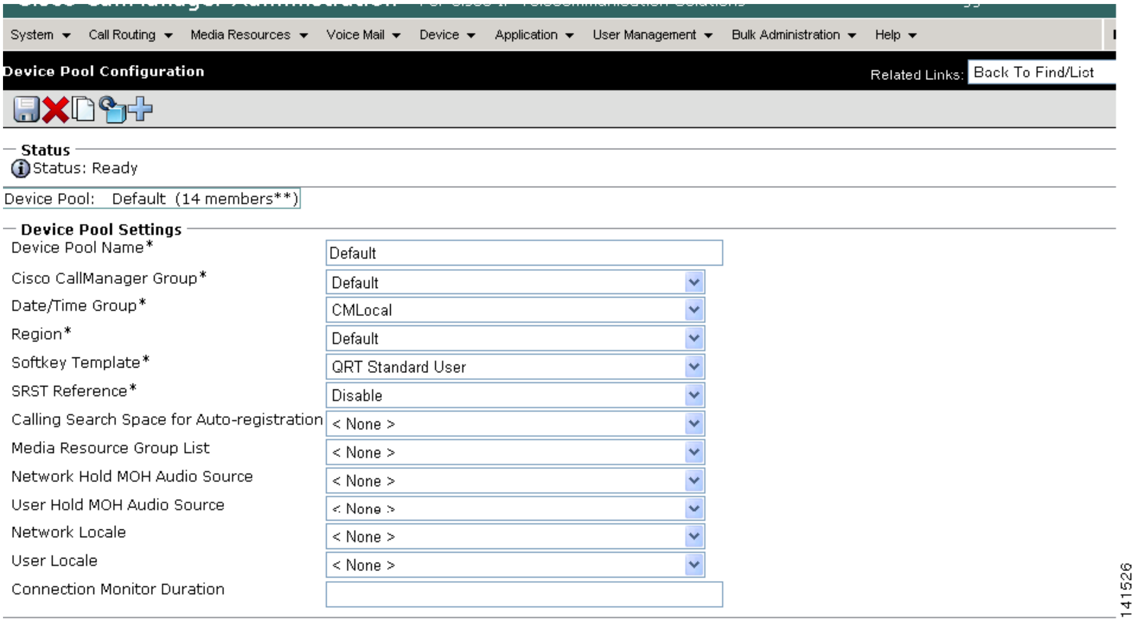
Step 3 Choose the Default device pool or any previously created device pool that displays.

You can add the template to the default device pool if you want all users to have access to the QRT softkey, or you can create a customized device pool for QRT feature users.

Step 4 In the Softkey Template field, choose the softkey template that contains the QRT softkey from the drop-down list box. (If you have not created this template, see the "Creating a Softkey Template with the QRT Softkey" section on page 18-16.)

Figure 18-13 shows an example of the Cisco CallManager Administration Device Pool Configuration window.

Figure 18-13 Device Pool Configuration



Device Pool Configuration

Status

Status: Ready

Device Pool: Default (14 members**)

Device Pool Settings

Device Pool Name*	Default
Cisco CallManager Group*	Default
Date/Time Group*	CMLocal
Region*	Default
Softkey Template*	QRT Standard User
SRST Reference*	Disable
Calling Search Space for Auto-registration	< None >
Media Resource Group List	< None >
Network Hold MOH Audio Source	< None >
User Hold MOH Audio Source	< None >
Network Locale	< None >
User Locale	< None >
Connection Monitor Duration	

Note All IP phones that are part of this device pool inherit this softkey template to provide an easy way for you to assign softkey templates to multiple phones. To associate softkey templates to individual IP phones, see the "Adding the QRT Softkey Template in Phone Configuration" section on page 18-20.

Step 5 Click **Save**.

Additional Information

See the "Related Topics" section on page 18-32.

Adding the QRT Softkey Template in Phone Configuration

Perform the following procedure to add the QRT softkey template to each user phone.

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Phone**.

The Find and List Phones window displays.

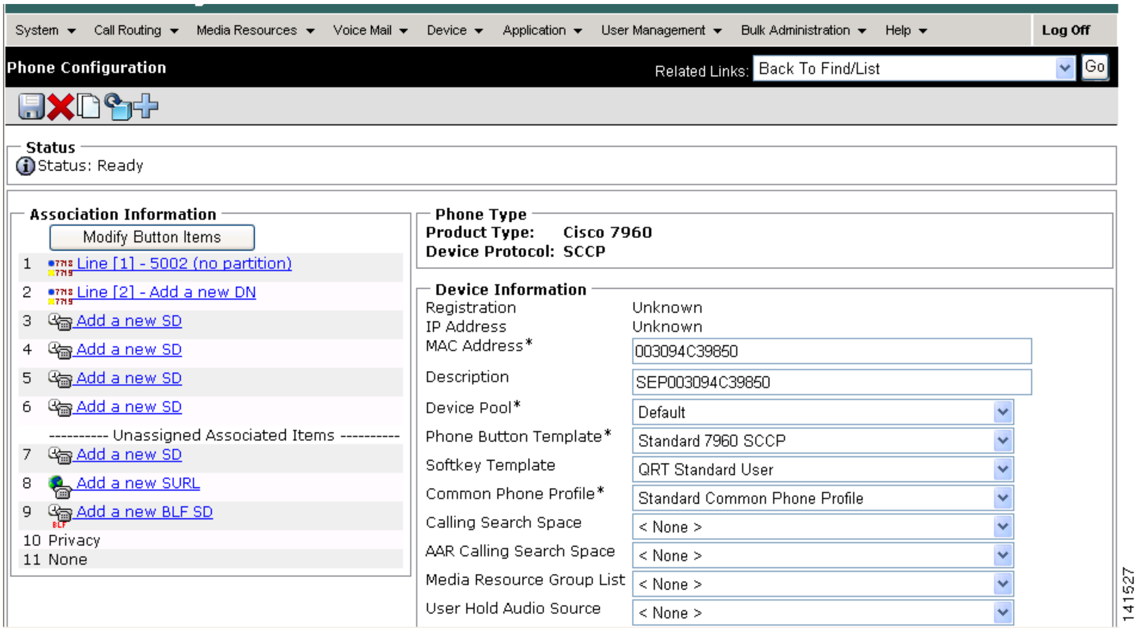
Step 2 Find the phone to which you want to add the softkey template. Refer to the "Finding a Phone" section of the Cisco IP Phone Configuration chapter in the *Cisco CallManager Administration Guide*.

Step 3 In the Softkey Template field, choose the softkey template that contains the QRT softkey from the drop-down list box. (If you have not created this template, see the "Creating a Softkey Template with the QRT Softkey" section on page 18-16.)

If you alternatively configured the softkey template in the device pool, from the Device Pool field, choose the device pool that contains the new softkey template.

Figure 18-14 shows an example of the Cisco CallManager Administration Phone Configuration window.

Figure 18-14 Phone Configuration



Phone Configuration

Related Links: Back To Find/List

Status
Status: Ready

Association Information

1	Line [1] - 5002 (no partition)
2	Line [2] - Add a new DN
3	Add a new SD
4	Add a new SD
5	Add a new SD
6	Add a new SD
	---------- Unassigned Associated Items ----------
7	Add a new SD
8	Add a new SURL
9	Add a new BLF SD
10	Privacy
11	None

Phone Type
Product Type: Cisco 7960
Device Protocol: SCCP

Device Information

Registration	Unknown
IP Address	Unknown
MAC Address*	003094C39850
Description	SEP003094C39850
Device Pool*	Default
Phone Button Template*	Standard 7960 SCCP
Softkey Template	QRT Standard User
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold Audio Source	< None >

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 18-32.

Configuring the Cisco CallManager Serviceability Features

The Cisco Extended Functions service uses the following Cisco CallManager Serviceability features:

- Service Activation—Configured from the Cisco CallManager Serviceability Tools window.
- SDI Trace—Configured from the Cisco CallManager Serviceability Trace Configuration window.
- Alarm Interface—Configured from the Cisco CallManager Serviceability Alarm Configuration window.
- Real-Time Monitoring Tool (RTMT)—Used to monitor the operating status of QRT and CTIManager. For detailed information about RTMT, refer to the *Cisco CallManager Serviceability Administration Guide*.

This section describes how to activate and configure the Cisco CallManager Serviceability features for use with QRT and contains the following information:

- Activating the Cisco Extended Functions Service for QRT, page 18-22
- Configuring Alarms and Traces for QRT, page 18-23

For additional information about Cisco CallManager Serviceability, refer to the *Cisco CallManager Serviceability Administration Guide.*

Activating the Cisco Extended Functions Service for QRT

Follow this procedure to activate the Cisco Extended Functions service for use with the QRT feature.

Note A link to Cisco CallManager Serviceability displays after you click the Show Navigation link on Cisco CallManager Administration.

Procedure

Step 1 From the Navigation drop-down list box in Cisco CallManager Administration, located in the upper, right corner of the window, choose Serviceability and click **Go**.

The Cisco CallManager Serviceability window displays.

Step 2 To activate the Cisco Extended Functions service, choose **Tools > Service Activation**.

A Server drop-down list box displays.

Step 3 From the Server drop-down list box, choose the Cisco CallManager server on which you want to activate the Cisco Extended Functions service.

Step 4 Check the **Cisco Extended Functions** check box.

Step 5 Click **Save**.

The CEF activation status changes from deactivated to activated.

Tip You can check the activation status of the Cisco Extended Functions service from Cisco CallManager Serviceability by choosing **Tools > Control Center - Feature Services**. Look for Cisco Extended Functions; if the Cisco Extended Functions service is active, it displays as Activated.

Additional Information

See the "Related Topics" section on page 18-32.

Configuring Alarms and Traces for QRT

Follow these procedures to configure alarms and SDI traces through Cisco CallManager Serviceability.

Procedure—Alarm Configuration

Step 1 From the Cisco CallManager Serviceability window, choose **Alarm > Configuration**.

A Server drop-down list box displays.

Step 2 From the Server drop-down list box, choose the Cisco CallManager server on which you want to configure alarms.

Step 3 From the Service drop-down list box, choose **Cisco Extended Functions**.

Step 4 Check the **Enable Alarm** check box for both Local Syslogs and SDI Trace.

Step 5 From the drop-down list box, configure the Alarm Event Level for both Local Syslogs and SDI Trace by choosing one of the following options:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

The default value specifies Error.

Step 6 Click **Save**.

Procedure—Trace Configuration

Step 1 From the Cisco CallManager Serviceability window, choose **Trace > Configuration**.

A Server drop-down list box displays.

Step 2 From the Server drop-down list box, choose the Cisco CallManager server on which you want to configure traces.

Step 3 From the Service drop-down list box, choose **Cisco Extended Functions**.

Step 4 Check the following check boxes:

- **Trace On**
- **Cisco Extended Functions Trace Fields**

Step 5 From the drop-down list box, configure the Debug Trace Level by choosing one of the following options:

- Error
- Special
- State Transition

- Significant
- Entry_exit
- Arbitrary
- Detailed

The default value specifies Error.

Note Cisco recommends that you check all the check boxes in this section for troubleshooting purposes.

Step 6 Click **Save**.

For additional information about configuring alarms and traces, refer to the *Cisco CallManager Serviceability Administration Guide*.

Setting the Cisco Extended Functions Service Parameters for QRT

Follow this procedure to set the Cisco Extended Functions service parameters by using Cisco CallManager Administration.

Note Cisco recommends that you use the default service parameters settings unless the Cisco Technical Assistance Center (TAC) instructs otherwise.

Procedure

Step 1 If your display shows the Cisco CallManager Serviceability window, from the Navigation drop-down list box, located in the upper, right corner of the window, choose CCM Administration and click **Go**.

The Cisco CallManager Administration window displays.

Step 2 From the Cisco CallManager Administration window, choose **System > Service Parameters**.

A Server drop-down list box displays.

Step 3 From the Server drop-down list box, choose the Cisco CallManager server where the QRT application resides.

A Service drop-down list box displays.

Step 4 From the Service drop-down list box, choose the Cisco Extended Functions service.

Step 5 Configure the following Cisco Extended Functions service parameters for QRT.

a. **Display Extended QRT Menu Choices**—Determines whether extended menu choices are presented to the user. You can choose one of the following configuration options:
   - Set this field to true to display extended menu choices (interview mode).
   - Set this field to false to not display extended menu choices (silent mode).
   - The recommended default value specifies false (silent mode).

b. **Streaming Statistics Polling Duration**—Determines the duration that is to be used for polling streaming statistics. You can choose one of the following configuration options:
   - Set this field to -1 to poll until the call ends.
   - Set this field to 0 to not poll at all.
   - Set it to any positive value to poll for that many seconds. Polling stops when the call ends.
   - The recommended default value specifies -1 (poll until the call ends).

c. **Streaming Statistics Polling Frequency (seconds)**— Designates the number of seconds to wait between each poll:
   - The value ranges between 30 and 3600.
   - The recommended default value specifies 30.

d. **Maximum No. of Files**—Specifies the maximum number of files before the file count restarts and overwrites the old files:
   - The value ranges between 1 and 10000.
   - The recommended default value specifies 250.

e. **Maximum No. of Lines per File**—Specifies the maximum number of lines in each file before starting the next file:
   - The value ranges between 100 and 2000.
   - The recommended default value specifies 2000.

Step 6 To configure a secure TLS connection to CTI, configure the following service parameters.

f. **CAPF Profile Instance ID for Secure Connection to CTI Manager—**Specifies the Instance ID of the Application CAPF Profile for application user CCMQRTSysUser that the Cisco Extended Function service will use to open a secure connection to CTI Manager. You must configure this parameter if CTI Manager Connection Security Flag is enabled.

Note Remember to turn on security by enabling the CTI Manager Connection Security Flag service parameter. You must restart the Cisco Extended Functions service for the changes to take effect.

See the "Securing a TLS Connection to CTI" section on page 18-7 for information on configuring the Application CAPF Profile.

g. **CTI Manager Connection Security Flag—**Indicates whether security for Cisco Extended Functions service CTI Manager connection is enabled or disabled. If enabled, Cisco Extended Functions will open a secure connection to CTI Manager using the Application CAPF Profile configured for the Instance ID for application user CCMQRTSysUser.

- The value choices are True and False.
- You must choose True to enable a secure connection to CTI.

Step 7 Click **Save**.

Additional Information

See the "Related Topics" section on page 18-32.

Using the QRT Viewer

You can use the QRT Viewer to view the IP phone problem reports that the Quality Report Tool generates. The QRT Viewer allows you to filter, format, and view the tool-generated phone problem reports, so they provide you with the specific information that you need.

- To view the QRT Viewer application, you need to install the Cisco Real-Time Monitoring Tool (RTMT) plug-in, which includes the trace collection feature.
- The trace collection feature enables collection and viewing of log files; the QRT Viewer is included with the trace collection feature.
- You can use the client application on Windows- or non-Windows-based operating systems.

Note For detailed information about installing and configuring the RTMT and trace collection feature, and for detailed information about accessing, configuring, using, and customizing the QRT Viewer for IP phone problem reports, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Additional Information

See the "Related Topics" section on page 18-32.

QRT Reports

QRT collects information from various sources, such as the source IP phone, the destination IP phone, the Cisco RIS Data Collector, Cisco CallManager, and the user. (The system does not collect information from gateways or other devices.) "Source" and "destination" in this case, do not refer to the calling party and called party in a connected call.

Note Refer to the QRT Viewer chapter in the *Cisco CallManager Serviceability Administration Guide* for additional information about QRT reports.

The following list provides information, segmented by information source, about the QRT report fields:

Information Collected from the Source Device

- Directory number of source device (in the case of multiline devices, the information shows only the first primary directory number)
- Source device type (for example, CP-7960, CP-7940)
- Source stream1 port number
- Source codec (for example, G.711u)
- Source packets (for example, 2,45,78)
- Source rcvr packets (for example, 12,45,78)
- Source rcvr jitter (for example, 0 0)
- Source rcvr packet lost (for example, 0,21 0,21)
- Source sampling timestamp, implicit (for example, 12:30, 13:00, 13:30, 14:00)

- Destination device name (IP)
- Destination stream1 port number

Note The number of samples that are collected for packets, jitter, packets lost, and so on, depends on the sampling duration and polling frequency. The streaming information gets collected only one time per call. For example, if phone A called phone B and both phone A and phone B submit multiple reports for the same call, only the first report includes the streaming data. Also, for the "Problems with last call" category, these values might reflect only the last snapshot of the streaming statistics that are stored in the phone device.

Information Collected from the Destination Device

The system collects the following information if the destination device is a supported Cisco IP Phone within same Cisco CallManager cluster. If the destination device is not an IP phone, the information includes only IP address, device name, and device type.

- Directory number of destination device (in the case of multiline devices, the information shows only the first primary directory number)
- Destination device type (for example, CP-7960, CP-7940)
- Destination codec
- Destination packets
- Destination rcvr packets
- Destination rcvr jitter
- Destination rcvr packet lost
- Destination sampling timestamp (Implicit)

Note The number of samples that are collected for packets, jitter, packets lost, and so on, depends on the sampling duration and polling frequency. The streaming information gets collected only one time per call. For example, if phone A called phone B and both phone A and phone B submit multiple reports for the same call, only the first report includes the streaming data that is included. QRT attempts to collect the information from the destination IP phone only for the "Problems with current call" category.

Information Collected from RIS Data Collector

- Source device owner (user name that is currently logged in to the IP phone; if no explicitly logged-in user exists, this field specifies null)
- IP address for source device
- Registered Cisco CallManager name for source device
- Source device type (if the device is not one of the supported IP phones; for example, RISCLASS_PHONE, RISCLASS_GATEWAY, RISCLASS_H323, RISCLASS_CTI, RISCLASS_VOICEMAIL)
- Source device model (for example, DBLTypeModel::MODEL_TELECASTER_MGR, DBLTypeModel::MODEL_TELECASTER_BUSINESS)
- Source device product (for example, DBLTypeProduct::PRODUCT_7960, DBLTypeProduct::PRODUCT_7940)
- Destination device name

- Destination device type (if the device is not one of the supported IP phones; for example, RISCLASS_PHONE, RISCLASS_GATEWAY, RISCLASS_H323, RISCLASS_CTI, RISCLASS_VOICEMAIL)
- Destination device model (for example, DBLTypeModel::MODEL_TELECASTER_MGR, DBLTypeModel::MODEL_TELECASTER_BUSINESS)
- Destination device product (for example, DBLTypeProduct::PRODUCT_7960, DBLTypeProduct::PRODUCT_7940)
- Registered Cisco CallManager name for destination device
- Destination device owner (user name that is currently logged in to the IP phone; if no explicitly logged-in user exists, this field specifies null)

Information Collected from Cisco CallManager/CTIManager

- Source device name (MAC address)
- CallingPartyNumber (the party who placed the call; for transferred calls, the transferred party becomes the calling party)
- OriginalCalledPartyNumber (the original-called party after any digit translations occurred)
- FinalCalledPartyNumber (for forwarded calls, this specifies the last party to receive the call; for non-forwarded calls, this field specifies the original called party)
- LastRedirectDn (for forwarded calls, this field specifies the last party to redirect the call; for non-forwarded calls, this field specifies the last party to redirect, via transfer or conference, the call)
- globalCallID_callManagerId (this field distinguishes the call for CDR Analysis and Reporting (CAR))
- globalCallID_callId (this field distinguishes the call for CAR)
- CallState (Connected, Connected Conference, Connected Transfer, On Hook)

Information Collected from the Cisco CallManager Database

- Sampling duration - Service parameter (for example, 50 seconds)
- Sampling frequency - Service parameter (for example, 30 seconds)
- Cluster ID - Enterprise parameter

Information Collected from the User

- Category
- ReasonCode
- TimeStamp (Implicit)

Table 18-6 shows the available fields for each supported category.

Note The following QRT report fields will display appropriate phone model and product names (for example, SCCP Phone): Source Model, Source Product, Destination Model, Destination Product, and CallState.

Table 18-6 QRT Fields by Supported Category

Information Source	Problems with Current Call	Problems with Last Call	Phone Recently Rebooted	Can't Make Calls
Source Device Name	X	X	X	X
DN of Source Device	X	X	X	X
IP Address of Source Device	X	X	X	X
Source Device Type	X	X	X	X
Source Device Owner	X	X	X	X
Registered Cisco CallManager for Source Device	X	X	X	X
Source Model	X	X	X	X
Source Product	X	X	X	X
Source Stream 1 Port Number	X	X		
Source Codec	X	X		
Source Packets	X	X		
Source Rcvr Packets	X	X		
Source Rcvr Jitter	X	X		
Source Rcvr Packet Lost	X	X		
Source Sampling Timestamp	X			
Destination Device Name	X	X		
DN of Destination Device	X	X		
IP Address of Destination Device	X	X		
Destination Device Type	X	X		
Destination Stream 1 Port Number	X			
Destination Codec	X			
Destination Packets	X			
Destination Rcvr Packets	X			
Destination Rcvr Jitter	X			
Destination Rcvr Packet Lost	X			
Destination Sampling Timestamp	X			
Destination Device Owner	X	X		
Registered Cisco CallManager for Destination Device	X	X		
Destination Model	X	X		
Destination Product	X	X		
Calling Party Number	X			

Table 18-6 QRT Fields by Supported Category (continued)

Information Source	Problems with Current Call	Problems with Last Call	Phone Recently Rebooted	Can't Make Calls
Original Called Party Number	X			
Final Called Party Number	X			
Last Redirect DN	X			
globalCallID_callManagerId	X			
globalCallID_callId	X			
Sampling Duration	X	X	X	X
Sampling Frequency	X	X	X	X
Cluster ID	X	X	X	X
Category	X	X	X	X
Reason Code	X	X		X
TimeStamp When Report is Submitted	X	X	X	X
sProtocol **Note** sProtocol represents the source destination protocol for the phones. This protocol has a value of 1 for SCCP phones, 2 for SIP phones, and 0 for UNKNOWN.	X	X	X	X
dProtocol **Note** dProtocol represents the destination protocol for the phones. This protocol has a value of 1 for SCCP phones, 2 for SIP phones, and 0 for UNKNOWN.	X	X		

Additional Information

See the "Related Topics" section on page 18-32.

Providing Information to Users for the QRT Feature

The Cisco IP Phone guides provide procedures for how to use the QRT feature on the Cisco IP Phone. For more information, refer to the following URL for the appropriate Cisco IP Phone Guide for your phone model:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm.

Additional Information

See the "Related Topics" section on page 18-32.

Troubleshooting the QRT Feature

Cisco CallManager Serviceability provides web-based tools to assist in troubleshooting Cisco CallManager problems. Use the Cisco CallManager Serviceability Trace Configuration, Alarm Configuration, and Real-Time Monitoring Tool to help troubleshoot problems with QRT. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

The Trace and Alarm tools work together. You can configure trace and alarm settings for Cisco CallManager services and direct alarms to local Syslogs or system diagnostic interface (SDI) log files. (SDI log files are viewable in text format only.)

You can set up traces for Cisco CallManager services on debug levels, specific trace fields, and Cisco CallManager devices such as phones or gateways. You can also perform a trace on the alarms that are sent to the SDI trace log files.

Use the trace collection feature to collect trace files and to analyze trace data for troubleshooting problems. (The trace collection feature includes the QRT Viewer.)

The trace collection feature provides three main functions:

- Configure trace parameters
- Collect trace files
- Analyze trace data for troubleshooting problems

Note Enabling Trace decreases system performance; therefore, enable Trace only for troubleshooting purposes. For assistance in using Trace, contact Cisco TAC.

Troubleshooting Tips

The following examples provide some common problems and recommended actions when troubleshooting scenarios for QRT:

Problem The QRT softkey is not available.

Solution Ensure that you have created, configured, and assigned the softkey template to enable the QRT feature.

Problem The QRT softkey is not working.

Solution Ensure that the Cisco Extended Functions service, Cisco CallManager, Cisco CTIManager, and Cisco RIS Data Collector services are operational.

Problem The QRT report does not include data.

Solution The system collects data from various sources, such as the user, source IP phone, destination IP phone, RIS Data Collector, Cisco CallManager, and Cisco CallManager databases. Check to make sure that the destination device is a supported IP phone and not a gateway or other unsupported device; otherwise, the system does not collect data from the destination device.

Note For more information about Cisco CallManager Serviceability tools, refer to the *Cisco CallManager Serviceability Administration Guide.*

For information about troubleshooting Cisco CallManager, refer to the *Troubleshooting Guide for Cisco CallManager.*

Additional Information

See the "Related Topics" section on page 18-32.

Related Topics

- Softkey Template Configuration, *Cisco CallManager Administration Guide*
- Device Pool Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phones, *Cisco CallManager System Guide*
- Device Defaults Configuration, *Cisco CallManager Administration Guide*
- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco CallManager Administration Guide*
- *Cisco CallManager System Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Security Guide*
- *Troubleshooting Guide for Cisco CallManager*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- Cisco IP Telephony Locale Installer
- Cisco IP Phone Guides

External Call Transfer Restrictions

External Call Transfer Restrictions feature allows the Cisco CallManager administrator to configure gateways, trunks, and route patterns as OnNet (internal) or OffNet (external) devices at the system level. By setting the devices as OffNet, administrators can restrict the transferring of an external call to an external device and thus help prevent toll fraud.

This chapter provides the following information about external call transfer restrictions:

- Introducing External Call Transfer Restrictions, page 19-1
- System Requirements for External Call Transfer Restrictions, page 19-4
- Interactions and Restrictions, page 19-4
- Installing and Activating External Call Transfer Restrictions, page 19-5
- Configuring External Call Transfer Restrictions, page 19-6
- Related Topics, page 19-9

Introducing External Call Transfer Restrictions

External call transfer restrictions block call transfer between external parties. Setting service parameters and configuring gateways, trunks, and route patterns as OffNet (external) devices provide external call transfer blocking. This feature provides an OnNet or OffNet alerting tone to the terminating end of the call (determined by the configuration of the device as either OnNet or OffNet, respectively). This chapter uses the following terms:

OnNet Device—A device that is configured as OnNet and considered to be internal to the network.

OffNet Device—A device that is considered as OffNet and, when routed, is considered to be external to the network.

Network Location—The location of the device, which is considered as OnNet or OffNet, with respect to the network.

Originating End—The device that gets transferred. The system considers this device as OnNet or OffNet.

Terminating End—The device that receives the transferred call. The system considers this device as OnNet or OffNet.

Incoming Call—A call for which only gateways and trunks call classification settings get used to classify it as OnNet or OffNet. Route Pattern call classification settings do not apply.

Outgoing Call—A call for which the call classification setting of the trunk, gateway, and route pattern gets considered. The Allow Device Override setting on the route pattern determines whether the trunk or gateway call classification setting gets used instead of the route pattern call classification setting.

Gateways and Trunks

You can configure gateways and trunks as OnNet (internal) or OffNet (external) by using Gateway Configuration or Trunk Configuration or by setting a clusterwide service parameter. When the feature is used in conjunction with the clusterwide service parameter Block OffNet to OffNet Transfer, the configuration determines whether calls can transfer over a gateway or trunk.

You can configure the following devices as internal and external to Cisco CallManager:

- H.323 gateway
- MGCP FXO trunk
- MGCP T1/E1 trunk
- Intercluster trunk
- SIP trunk

Route Patterns

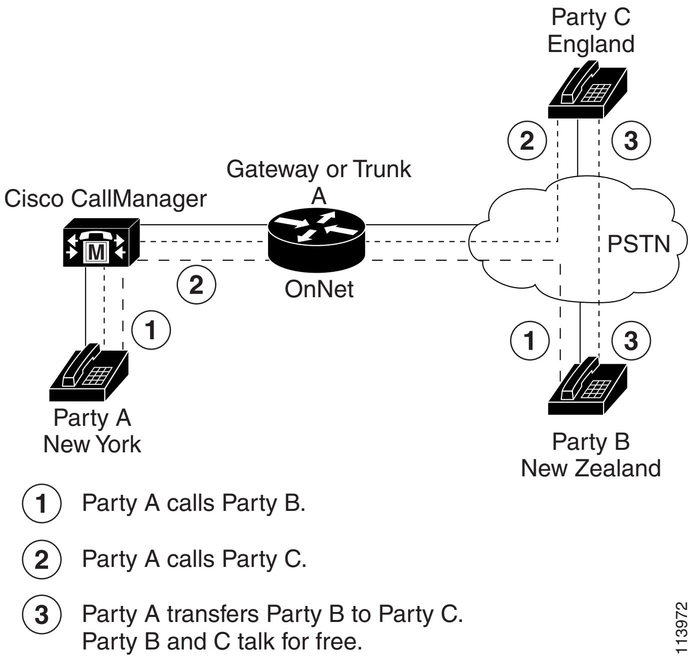
To classify a call as OnNet or OffNet, administrators can set the Call Classification field to OnNet or OffNet, respectively, on the Route Pattern Configuration window. Administrators can override the route pattern setting and use the trunk or gateway setting by checking the Allow Device Override check box on the Route Pattern Configuration window.

For more information, see the "Configuring External Call Transfer Restrictions" section on page 19-6.

Example

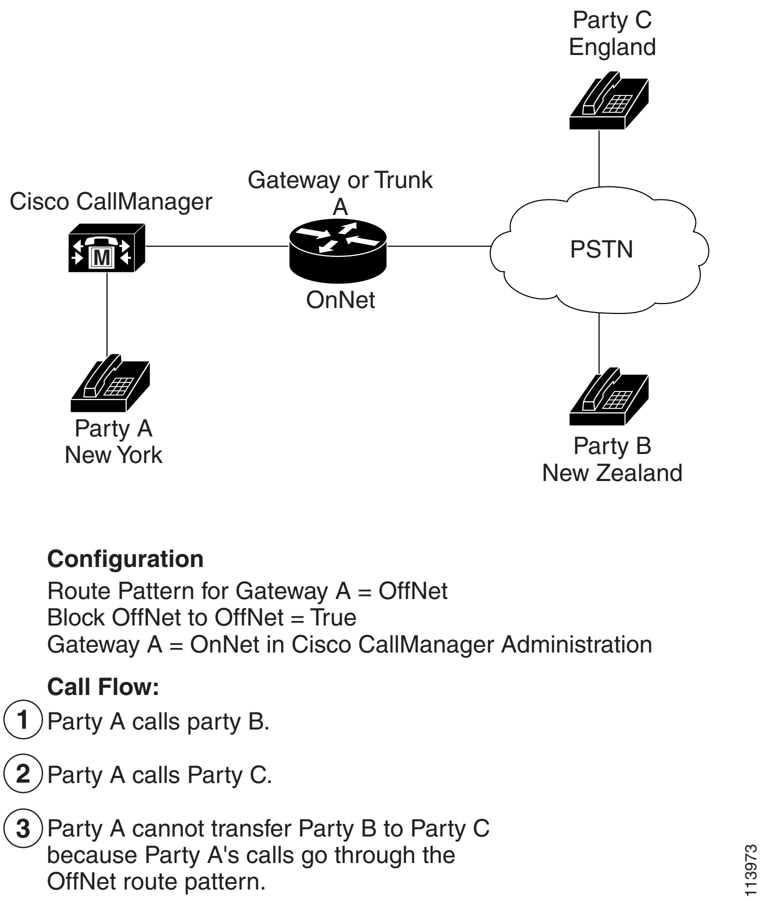
The following example illustrates how callers use transfer to avoid paying for long-distance calls. In Figure 19-1, Party A from ABC Company in New York calls Party B, a friend in New Zealand. After the call connects, Party A transfers the call to Party C, another friend who lives in England. When transfer completes, Party B and Party C are connected, and Party A gets disconnected. As a result, ABC Company gets billed for the call between New Zealand and England.

Figure 19-1 Transferring External Calls to an External Party



In Figure 19-2, the system prevents transferring an external call to an external party because, regardless of how the gateway or trunk is configured, the route pattern was configured as OffNet, and the service parameter Block OffNet to OffNet Transfer is set to True.

Figure 19-2 Blocking an External Call from Transferring to an External Party



Configuration
Route Pattern for Gateway A = OffNet
Block OffNet to OffNet = True
Gateway A = OnNet in Cisco CallManager Administration

Call Flow:

1 Party A calls party B.

2 Party A calls Party C.

3 Party A cannot transfer Party B to Party C because Party A's calls go through the OffNet route pattern.

System Requirements for External Call Transfer Restrictions

The external call transfer restriction requires the following software component to operate:

- Cisco CallManager 5.0

Interactions and Restrictions

The following sections describe the interactions and restrictions for external call transfer restrictions:

- Interactions, page 19-5
- Restrictions, page 19-5

Interactions

The following sections describe how external call transfer restrictions feature interacts with Cisco CallManager applications and call processing.

Drop Conference

The Drop Conference feature determines whether an existing ad hoc conference should be dropped by checking whether the conference parties are configured as OffNet or OnNet. You use the service parameter Drop Ad Hoc Conference and choose the option When No OnNet Parties Remain in the Conference to configure the feature. You determine OnNet status for each party by checking the device or route pattern that the party is using. For more information, refer to "Ad Hoc Conference Settings" in the *Cisco CallManager System Guide*.

Bulk Administration

Bulk Administration inserts gateway configuration (OffNet or OnNet) on the Gateway Template. Refer to the *Cisco CallManager Bulk Administration Guide* for more information.

Dialed Number Analyzer (DNA)

When used to perform digit analysis on a gateway, DNA displays the Call Classification that is configured for the gateway and the route pattern. Refer to the *Cisco CallManager Dialed Number Analyzer Guide* for more information.

Restrictions

The following restrictions apply to external call transfer restrictions:

- FXS gateways such as Cisco Catalyst 6000 24 Port do not have a Call Classification field on the Gateway Configuration window; therefore, the system always considers them as OnNet.
- The system does not support the Cisco VG-248 Gateway which does not have a Call Classification field.
- Cisco CallManager considers all Cisco IP Phones and FXS ports as OnNet (internal) that cannot be configured as OffNet (external).

Installing and Activating External Call Transfer Restrictions

To activate external call transfer restrictions, perform the following steps:

1. Set the Block OffNet to OffNet Transfer service parameter to True.
2. In Route Pattern Configuration window, set the Call Classification field to OffNet. Leave the Allow Device Override check box unchecked, so the device uses the Call Classification setting of the route pattern.
3. Configure the trunks and gateways that you want to be identified as OffNet.

See the "External Call Transfer Restrictions Configuration Checklist" section on page 19-6 for details.

Configuring External Call Transfer Restrictions

This section contains the following information:

- External Call Transfer Restrictions Configuration Checklist, page 19-6
- Configuring External Call Transfer Restrictions Service Parameters, page 19-7
- Configuring Transfer Capabilities by Using Gateway Configuration, page 19-7
- Configuring Transfer Capabilities by Using Trunk Configuration, page 19-8
- Configuring Transfer Capabilities by Using Route Pattern Configuration, page 19-8

External Call Transfer Restrictions Configuration Checklist

Table 19-1 provides a checklist to configure external call transfer restrictions.

Table 19-1 External Call Transfer Restrictions Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	To block external calls from being transferred to external devices, perform the following steps: **1.** Set the Block OffNet to OffNet Transfer clusterwide service parameter to True. **2.** For incoming calls, configure individual gateways or trunks as OffNet. **3.** For outgoing calls, configure route pattern Call Classification field as OffNet. The Allow Device Override check box can be checked or unchecked, depending on the requirements (for example, if the check box is checked, the setting on the associated gateway or trunk is considered; if it is unchecked, the call classification value of the route pattern classifies the call).	Setting the Block OffNet to OffNet Transfer Service Parameter, page 19-7 *Configuring Transfer Capabilities by Using Gateway Configuration, page 19-7* Configuring Transfer Capabilities by Using Trunk Configuration, page 19-8 Configuring a Route Pattern, *Cisco CallManager Administration Guide*
Step 2	To configure all gateways or trunks to be OffNet (external) or OnNet (internal), perform the following steps: **1.** Set the Cisco CallManager clusterwide service parameter Call Classification to OffNet (if all gateways and trunks are to be external) or OnNet (if all gateways and trunks are to be internal). **2.** Configure individual gateways or trunks to Use System Default in the Call Classification field.	Configuring Transfer Capabilities by Using Call Classification Service Parameter, page 19-7 Configuring Transfer Capabilities by Using Gateway Configuration, page 19-7 Configuring Transfer Capabilities by Using Trunk Configuration, page 19-8
Step 3	On the Route Pattern Configuration window, set the Call Classification field as OffNet. The Allow Device Override check box can be checked or unchecked, depending on the requirements and the configurations of the gateway or trunk.	Configuring a Route Pattern, *Cisco CallManager Administration Guide*

Configuring External Call Transfer Restrictions Service Parameters

You can set two service parameters for the external call transfer restrictions feature: Call Classification and Block OffNet to OffNet Transfer. The following sections provide configuration information:

- Configuring Transfer Capabilities by Using Call Classification Service Parameter, page 19-7
- Setting the Block OffNet to OffNet Transfer Service Parameter, page 19-7

Configuring Transfer Capabilities by Using Call Classification Service Parameter

To configure all gateways or trunks in the Cisco CallManager cluster to be OffNet (external) or OnNet (internal), perform the following two steps:

1. Using the Cisco CallManager clusterwide service parameter Call Classification, choose either OffNet or OnNet (the default specifies OffNet).
2. In the Call Classification field on the Gateway Configuration and Trunk Configuration windows, configure each gateway and trunk to Use System Default (this reads the setting in the Call Classification service parameter and uses that setting for the gateway and trunk).

Additional Information

See the "Related Topics" section on page 19-9.

Setting the Block OffNet to OffNet Transfer Service Parameter

The Cisco CallManager clusterwide service parameter Block OffNet to OffNet Transfer allows administrators to prevent users from transferring external calls to another external number. This parameter specifies values as True or False. Setting the parameter to True blocks external calls from being transferred to another external device. The default value specifies False. You modify the Block OffNet to OffNet Transfer service parameter by using the Service Parameters Configuration window.

When a user tries to transfer a call on an OffNet gateway or trunk when the service parameter Block OffNet to OffNet Transfer is set to True, a message displays on the user phone to indicate that the call cannot be transferred.

Additional Information

See the "Related Topics" section on page 19-9.

Configuring Transfer Capabilities by Using Gateway Configuration

To configure the gateway as OffNet, OnNet, or Use System Default, perform the following procedure. The system considers calls that come to the network through that gateway as OffNet or OnNet, respectively.

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Gateway**.

The Find and List Gateways window displays.

Step 2 To list the configured gateways, click **Find**.

The gateways that are configured in Cisco CallManager display.

Step 3 Choose the gateway that you want to configure as OffNet or OnNet.

Step 4 In the Call Classification field, choose the setting. See Table 19-2 for a description of these settings.

Step 5 Click **Save**.

Configuring Transfer Capabilities by Using Trunk Configuration

To configure the trunk as OffNet, OnNet, or Use System Default, perform the following procedure. The system considers calls that come to the network through that trunk as OffNet or OnNet, respectively.

Procedure

Step 1 From Cisco CallManager Administration, choose **Device > Trunk**.

The Find and List Trunk window displays.

Step 2 To list the configured trunks, click **Find**.

The trunks that are configured in Cisco CallManager display.

Step 3 Choose the trunk that you want to configure as OffNet or OnNet.

Step 4 In the Call Classification field, choose the setting. See Table 19-2 for a description of these settings.

Step 5 Click **Save**.

Table 19-2 Call Classification Configuration Settings

Setting Name	Description
OffNet	This setting identifies the gateway as an external gateway. When a call comes in from a gateway that is configured as OffNet, the system sends the outside ring to the destination device.
OnNet	This setting identifies the gateway as an internal gateway. When a call comes in from a gateway that is configured as OnNet, the system sends inside ring to the destination device.
Use System Default	This setting uses the Cisco CallManager clusterwide service parameter Call Classification.

Configuring Transfer Capabilities by Using Route Pattern Configuration

The Route Pattern Configuration window provides the following fields:

- Call Classification—Use this drop-down list box to classify the call that uses this route Pattern as OffNet or OnNet.
- Provide Outside Dial Tone—If Call Classification is set to OffNet, this check box gets checked.
- Allow Device Override—When this check box is checked, the system uses the Call Classification setting of the trunk or gateway that is associated with the route pattern instead of the Call Classification setting on the Route Pattern Configuration window.

Additional Information

See the "Related Topics" section on page 19-9.

Related Topics

- Route Pattern Configuration, *Cisco CallManager Administration Guide*
- Gateway Configuration, *Cisco CallManager Administration Guide*
- Trunk Configuration, *Cisco CallManager Administration Guide*
- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- Conference Bridges, *Cisco CallManager System Guide*

Additional Cisco Documentation

- *Cisco CallManager Dialed Number Analyzer Guide*
- *Cisco CallManager Bulk Administration Guide*

CHAPTER 20

Presence

The Presence feature allows a user to monitor the real-time status of another user at a directory number or SIP URI.

This section covers the following topics:

- Introducing Presence, page 20-2
- Understanding How Presence Works with Phones and Trunks, page 20-2
- Understanding How Presence Works with Route Lists, page 20-4
- Understanding Presence Groups, page 20-4
- Understanding Presence Authorization, page 20-7
- Understanding How the SUBSCRIBE Calling Search Space Works, page 20-8
- Presence Feature Interactions/Restrictions, page 20-9
- Presence Configuration Checklist, page 20-10
- Configuring Presence Service Parameters and Enterprise Parameters, page 20-12
- Configuring and Applying the SUBSCRIBE Calling Search Space, page 20-13
- Finding Presence Groups, page 20-14
- Configuring Presence Groups, page 20-15
- Presence Group Configuration Settings, page 20-15
- Deleting a Presence Group, page 20-16
- Applying a Presence Group, page 20-17
- Presence Group and Presence Authorization Tips, page 20-18
- Configuring BLF/SpeedDial Buttons, page 20-19
- BLF/SpeedDial Configuration Settings, page 20-20
- Where to Find More Information, page 20-21

Introducing Presence

When you configure Presence in Cisco CallManager Administration, an interested party, known as a watcher, can monitor the real-time status of a directory number or SIP URI, a presence entity, from the device of the watcher.

Note A SIP URI comprises a call destination configured with a *user@host* format, such as **xten3@CompB.cisco.com** or **2085017328@10.21.91.156:5060**.

A watcher can monitor the status of the presence entity (also called presentity) with the following options:

- BLF/SpeedDial buttons
- Missed call, placed call, or received call lists in the directories window
- Shared directories, such as the corporate directory

Call lists and directories display the BLF status for existing entries.

Note You must configure BLF/SpeedDial buttons so the presence entity displays as a speed dial on the device of the watcher. For presence-supported SIP phones, you can configure directory numbers or SIP URIs as BLF/SpeedDial buttons. For presence-supported SCCP phones, you can only configure directory numbers as BLF/SpeedDial buttons. The BLF value does not have to be on the cluster.

Watchers initiate presence requests (SUBSCRIBE messages) to obtain the status of presence entities in the cluster or outside of the cluster. The entity that is subscribed to responds with a response message (NOTIFY message), which carries the presence status.

Tip Administrators configure the phone features associated with presence: BLF/SpeedDials, call lists, or both. After administrators configure presence features, real-time status icons display on the watcher device to indicate whether the presence entity is on the phone, not on the phone, status unknown, and so on.

For information on the Busy Lamp Field (BLF) status icons that display on the phone, refer to the Cisco IP Phone documentation that supports your phone model.

To identify whether your phone model supports presence, refer to the Cisco IP Phone documentation that supports your phone model and this version of Cisco CallManager.

Understanding How Presence Works with Phones and Trunks

Tip Use the information in this section with the "Understanding Presence Groups" section on page 20-4, the "Understanding Presence Authorization" section on page 20-7, the"Understanding How Presence Works with Route Lists" section on page 20-4, and the "Understanding How the SUBSCRIBE Calling Search Space Works" section on page 20-8. The following information assumes that the phones and trunks have permission to view the status of the presence entity, as configured through presence groups.

Cisco CallManager handles all presence requests for Cisco CallManager users, whether inside or outside the cluster.

For a Cisco CallManager watcher that sends a presence request through the phone, Cisco CallManager responds with the presence status directly if the phone and presence entity are colocated.

If the device exists outside of the cluster, Cisco CallManager queries the external device through the SIP trunk.If the watcher has permission to monitor the external device, the SIP trunk sends the presence request to the external device and returns presence status to the watcher.

For non-Cisco CallManager watchers that send presence requests through a Cisco CallManager trunk, Cisco CallManager responds with presence status if Cisco CallManager supports the presence entity. If Cisco CallManager does not support the presence entity, the request gets rejected.

The following examples demonstrate how presence works for phones and trunks when the phones and trunks have permission to send and receive presence requests.

A Cisco CallManager User Queries the BLF Status of Another Cisco CallManager User.

A Cisco CallManager user calls another Cisco CallManager user only to find that the called party is not available. When available, the called party checks the missed call list, and the phone contacts Cisco CallManager. Cisco CallManager validates that the called party is a valid watcher and determines that the caller represents a Cisco CallManager presence entity. The BLF status for the caller gets updated on the phone of the called party.

A Cisco CallManager User Queries the BLF Status of a NonCisco CallManager User.

A non-Cisco CallManager user calls a Cisco CallManager user only to find that the Cisco CallManager user is unavailable. When available, the Cisco CallManager user checks the missed call list, and the phone contacts Cisco CallManager. Cisco CallManager confirms that the Cisco CallManager user is a valid watcher and determines that the nonCisco CallManager user represents a presence entity. A SIP trunk interacts with the non-Cisco CallManager network and Cisco CallManager, and status for the nonCisco CallManager user gets updated on the phone of the Cisco CallManager user.

A NonCisco CallManager User Queries the Presence Status of a Cisco CallManager User.

A nonCisco CallManager user queries the state of a Cisco CallManager user. The request comes through a Cisco CallManager SIP trunk. Cisco CallManager verifies that the nonCisco CallManager user is a valid watcher and determines that the Cisco CallManager user represents a Cisco CallManager presence entity. Cisco CallManager sends the status to phone of the nonCisco CallManager user.

A Cisco CallManager Accesses the Corporate Directory to Get BLF Status.

A Cisco CallManager user accesses the corporate directory on the phone. For each directory entry, BLF status displays.

A Phone Monitors a BLF/SpeedDial.

After an administrator configures the presence feature and the BLF/SpeedDial buttons, a user can immediately begin to monitor the real-time status of a presence entity.

Understanding How Presence Works with Route Lists

Tip Use the information in this section with the "Understanding How Presence Works with Phones and Trunks" section on page 20-2, the "Understanding Presence Groups" section on page 20-4, the "Understanding Presence Authorization" section on page 20-7, and the "Understanding How the SUBSCRIBE Calling Search Space Works" section on page 20-8.

Cisco CallManager receives presence requests from watchers and status responses from presence entities. Watchers and presence entities can exist inside the cluster or outside of the cluster.

Cisco CallManager supports external incoming and outgoing presence requests through the SIP trunk. SIP trunks can be members of route groups, which are members of route lists. When Cisco CallManager receives a presence request or notification status that is associated with an outbound SIP trunk or route group, Cisco forwards the request or status to a SIP trunk.

Note Presence requests and responses must route to SIP trunks or routes that are associated with SIP trunks. The system rejects presence requests routing to MGCP/H323 trunk devices.

When a request gets forwarded to a route group or list, any SIP trunk in the group or list can carry the request. Cisco CallManager forwards the request to the next available or idle outbound SIP trunk in the group or list. This process repeats until Cisco CallManager receives a successful response or the operation fails.

After the presence request to an external presentity is successful, the SIP trunk receives notification messages based on status changes for the presentity and sends the status to the route list/group to notify the watcher. When different watchers send presence requests to the same presentity that is reached through the route list/group and SIP trunk, Cisco CallManager sends the cached status for the presentity to the subscriber instead of creating another subscription.

The presentity can terminate the subscription at any time due to time-out or other reasons. When the SIP trunk receives a termination status, the termination status gets passed to the route list or group to notify the watcher.

Refer to the Route List Configuration chapter in the *Cisco CallManager Administration Guide* for more information about configuring route lists.

Understanding Presence Groups

Tip The Default Inter-Presence Group Subscription service parameter for the Cisco CallManager service sets the clusterwide permissions parameter for presence groups to *Allow Subscription* or *Disallow Subscription***.** This enables administrators to set a system default and configure presence group relationships by using the default setting for the cluster. For information on configuring this service parameter, see the "Configuring Presence Service Parameters and Enterprise Parameters" section on page 20-12.

Cisco CallManager allows you to configure presence groups to control the destinations that watchers can monitor. To configure a presence group, create the group in Cisco CallManager Administration and assign one or more destinations and watchers to the same group.

Note The system always allows presence requests within the same presence group.

You must also specify the relationships to other presence groups by using one of the following permissions from the drop-down list in the Presence Group Configuration window:

- **Use System Default**—To use the Default Inter-Presence Group Subscription service parameter (*Allow Subscription* or *Disallow Subscription*) setting for the permission setting, select the group(s) and configure the Subscription Permission to *Use System Default***.**
- **Allow Subscription**—To allow a watcher in this group to monitor members in another group, select the group(s) and configure the Subscription Permission setting to *Allow Subscription*.
- **Disallow Subscription**—To block a watcher in this group from monitoring members in another group, select the group(s) and configure the Subscription Permission setting to *Disallow Subscription*.

Tip Whenever you add a new presence group, Cisco CallManager defines all group relationships for the new group with the default cluster setting as the initial permission setting.To apply different permissions, you configure new permissions between the new group and existing groups and between existing groups and the new group for each permission that you want to change.

The permissions that are configured for a presence group display in the Presence Group Relationship pane. Permissions that use the system default permission setting for the group-to-group relationship do not display.

Example: Configuring Presence Group Permissions

Assume the clusterwide setting for Default Inter-Presence Group Subscriptions is set to Disallow. You create two presence groups: Group A (workers) and Group B (managers). If you want to allow Group B members to monitor Group A members but to block group A members from monitoring Group B members, you would configure *Allow* for Group B to Group A. (Because the system default is Disallow, Group A already disallows subscriptions to Group B, unless you change the Default Inter-Presence Group Subscriptions service setting.)

Cisco CallManager automatically creates the Standard Presence Group at installation, which serves as the default group for presence users. All presence users (except application user) initially get assigned to the Standard Presence group. You cannot delete this group.

Note Because not all application users use the SIP trunk or initiate presence requests, the default setting for application user specifies *None*. To assign an application user to the Standard Presence Group, administrators must configure this option.

For each presence group that you create, you apply the presence group to one or more of following items in Cisco CallManager Administration (refer to Table 20-1).

Table 20-1 Applying Presence Groups

Apply Presence Groups to	Presence Entity or Watcher	Comments
Directory number	Presence entity	For SIP or SCCP phones
Trunk	Watcher and Presence Entity	For external presence servers that send presence requests via SIP trunk or a proxy server that is connected on SIP trunk (serving as watcher) For outgoing presence requests to the SIP trunk (serving as presence entity)
Phone	Watcher	For SIP or SCCP phones
Application User	Watcher	For external applications that send presence requests via SIP trunk or home on a proxy server that is connected on SIP trunk (for example Web Dial, IPPM, Meeting Place, conference servers, and presence servers)
End User	Watcher	For user directories and call lists and to configure extension mobility settings.
Autogenerated device profile	Watcher	For phones with extension mobility support only

Note 1: A phone serves as a watcher; a line on a phone cannot serve as a watcher.

Note 2: It is not necessary to provision presence groups for BLF/SpeedDials.

Tip Refer to "Understanding Presence Authorization" section on page 20-7, for additional requirements for presence requests through the SIP trunk.

The following examples describe how a phone or trunk obtains the destination status by using different presence groups and permissions.

A Phone Wants Status About a Directory Number Assigned to BLF/SpeedDial.

Phone A has directory number 1111 (Phone B) configured as a BLF/SpeedDial button to monitor presence status for Phone B. Phone A and Phone B are colocated. Phone A receives real-time status for directory number 1111 and displays the status icon next to the BLF/SpeedDial button. The system does not invoke presence group authorization.

A Phone Wants Status About a Directory Number in a Call List.

Phone A, which has the presence group, User Group, configured for it, has directory number 1111 in the Missed Calls call list. Directory number 1111, which exists for Phone B, has the presence group, Executive Group, configured for it. The Presence Group Configuration window indicates that the relationship between the User Group and Executive Group is Disallowed, as specified in the Presence Group Relationship pane. Phone A cannot receive real-time status for directory number 1111, and Phone A does not display the real-status icon next to the Missed Call list entry.

A SIP Proxy Server That Is Connected to a SIP Trunk Wants Status About a Cisco CallManager Directory Number.

The following example describes how a SIP trunk obtains the status of a directory number when different presence groups are configured for the SIP trunk and directory number. SIP proxy server D uses SIP trunk C to contact Cisco CallManager for the status of directory number 5555 because directory number 5555 exists as a BLF/SpeedDial button on SIP phone E, which connects to the proxy server. The SIP trunk indicates that it has presence group, Administrator Group, configured for it, and directory number 5555 is assigned to the Engineering Group. The Presence Group Configuration window indicates that the relationship between the Administrator Group and Engineering Group is allowed, as specified in the Presence Group Relationship pane. Cisco CallManager sends the status of the directory number to the trunk, which passes the status to the SIP proxy server D. SIP phone E receives real-time status for directory number 5555, and the phone displays the real-time status icon next to the BLF/SpeedDial button.

Understanding Presence Authorization

Tip Use the information in this section with the "Understanding How Presence Works with Phones and Trunks" section on page 20-2, the "Understanding Presence Groups" section on page 20-4, and the "Understanding How the SUBSCRIBE Calling Search Space Works" section on page 20-8.

To view the status of a presence entity, watchers send presence requests to Cisco CallManager. The system requires watchers to be authorized to initiate status requests for a presence entity by using these mechanisms:

- The watcher presence group must have authorization to obtain the status for the presence entity presence group, whether inside or outside of the cluster.
- Cisco CallManager must have authorization to accept presence requests from an external presence server or application.

Note The authorization process remains independent of calling search space routing for presence requests.

To initiate presence group authorization, you must configure one or more presence groups and assign the appropriate permissions. Administrators configure permission settings for presence groups, which specify when a watcher's presence group can monitor the status of members in other groups. To validate a presence request, Cisco CallManager performs a database lookup by using the permissions that are assigned to the presence groups that are configured.

If you choose not to use presence group authorization, leave all presence users assigned to the default presence group and do not configure additional groups or permissions. You will still need to configure authorization for a SIP trunk or application if you want to authorize Cisco CallManager to accept incoming presence requests from an external presence server or application.

Tip When an administrator decides to add or change a BLF/SpeedDial button, the administrator ensures that the watcher is authorized to monitor that destination.

Administrators configure the Cisco CallManager system to accept presence requests that come via the SIP trunk by configuring parameters for the SIP trunk and application user.

To authorize the Cisco CallManager system to accept incoming presence requests from the SIP trunk, check the Accept Presence Subscription check box in the SIP Trunk Security Profile window. (To block incoming presence requests on a SIP trunk, uncheck the check box.) When SIP trunk presence requests are allowed, Cisco CallManager accepts requests from the SIP user agent (SIP proxy server or external presence server) that connects to the trunk. Consider digest authentication as optional when Cisco CallManager is configured to accept presence requests from a SIP trunk.

Tip To use presence group authorization with incoming presence requests on a SIP trunk, configure a presence group for the trunk, such External_Presence_Serv_Group1, and configure the appropriate permissions to other groups inside the cluster.

To authorize the Cisco CallManager system to accept presence requests from an external application that connects on the SIP trunk, check the Enable Application Level Authorization check box in the SIP Trunk Security Profile GUI and the Accept Presence Subscription check box in the Applications User Configuration window for the application. When you configure the Cisco CallManager system to accept presence requests from an application user, Cisco CallManager validates each presence request that is received on the SIP trunk before accepting it.

Tip To use presence group authorization with incoming presence requests from a SIP trunk application, configure a presence group for the application, such as Presence_User, and configure the appropriate permissions to other groups inside the cluster.

If you configure both levels of authorization for SIP trunk presence requests, the presence group for the SIP trunk gets used only when no presence group is identified in the incoming request for the application.

Before application authorization can occur, Cisco CallManager must first authenticate the external application by using digest authentication. Enable Application Level Authorization cannot be checked unless Enable Digest Authentication is checked.

Note The authorization could pass for the trunk but fail for the application. Refer to "Presence Group and Presence Authorization Tips" section on page 20-18, for additional considerations when configuring presence authorization.

Refer to the *Cisco CallManager Security Guide* for more information about authentication and authorization.

Understanding How the SUBSCRIBE Calling Search Space Works

The SUBSCRIBE Calling Search Space determines how Cisco CallManager routes presence requests that come from the trunk or the phone. The SUBSCRIBE calling search space, associated with a watcher, specifies the list of partitions to search for routing information to a presence entity for presence requests.

To configure a calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces (Call Routing > Class Control > Calling Search Space). For information on how to configure a calling search space, refer to the "Calling Search Space Configuration" chapter in the *Cisco CallManager Administration Guide*.

The SUBSCRIBE Calling Search space option allows you to apply a calling search space separate from the call-processing Calling Search Space for presence requests. If you do not select a different calling search space for presence requests, the SUBSCRIBE Calling Search Space defaults to None.

You apply the SUBSCRIBE Calling Search Space to the SIP trunk, phone, end user, or autogenerated device profile (for phones with extension mobility support only). The SUBSCRIBE Calling Search Space associated with an end user gets used for extension mobility calls.

Understanding How Presence Works with Extension Mobility

Tip Use the information in this section in conjunction with the "Understanding Presence Groups" section on page 20-4, the "Understanding Presence Authorization" section on page 20-7, and the "Understanding How the SUBSCRIBE Calling Search Space Works" section on page 20-8.

When you configure BLF/SpeedDial buttons in a user device profile in Cisco CallManager Administration, a phone that supports Cisco CallManager Extension Mobility can display presence status on the BLF/SpeedDial buttons after you log in to the device. The SUBSCRIBE calling search space and presence group that are configured for the user apply.

When the extension mobility user logs out, a phone that supports Cisco CallManager Extension Mobility displays presence status on the BLF/SpeedDial buttons for the log-out profile that is configured:

- When a user device profile is configured for the logout profile, the SUBSCRIBE calling search space and presence group that are configured for the user apply.
- When an autogenerated device profile is generated for the logout profile, the SUBSCRIBE calling search space and presence group that are defined in the autogenerated profile apply.

Tip Refer to "Device Profile Configuration" in the *Cisco CallManager Administration Guide* for more information about configuring device profiles and updating autogenerated profiles.

Presence Feature Interactions/Restrictions

The following interactions and restrictions apply to the Presence feature:

- Cisco IP Manager Assistant does not support SIP presence.
- Cisco CallManager supports an inbound presence request to a directory number that is associated with a hunt list.
- Cisco CallManager rejects presence requests to a directory number that is associated with a hunt pilot.
- Because the administrator ensures that the watcher is authorized to monitor the destination when configuring a BLF/SpeedDial, presence group authorization does not apply to BLF/SpeedDials.

- For Cisco IP Phones with multiple lines, the phone uses the cached information that is associated with the line directory number for missed and placed calls to determine presence authorization. If this call information is not present, the phone uses the primary line as the subscriber for presence authorization. For BLF/SpeedDial buttons on Cisco IP Phones with multiple lines, the phone uses the first available line as the subscriber.
- When a user monitors a directory number configured for Cisco IP SIP Phone models 7960, 7940, 7905, and 7912, the system displays a status icon for ‘not on the phone‘ on the watcher device when the presentity is off-hook (but not in a call connected state). These phones do not detect an off-hook status. For all other phone types, the system displays the status icon for ‘on the phone‘ on the watcher device for an off-hook condition at the presentity.

The following restrictions apply to Presence BLF interaction with DNs on H.323 phones when the H.323 phone device serves as presentity:

- When the H.323 phone is in the RING IN state, the BLF status gets reported as Busy. (For SCCP and SIP phone presentities in the RING IN state, the BLF status gets reported as Idle.)
- When the H.323 phone is not connected to Cisco CallManager for any reason, such as the Ethernet cable is unplugged from the phone, the BLF status gets reported as Idle all the time. (For SCCP and SIP phone presentities that are not connected to Cisco CallManager, the BLF status gets reported as Unknown.)

Presence Configuration Checklist

Tip The following information assumes that the phones and SIP trunks exist in the Cisco CallManager database. For information on how to add a phone or SIP trunk, refer to the *Cisco CallManager Administration Guide*.

Table 20-2 provides tasks that you must perform to configure presence features:

- To configure the call list phone feature for presence, perform Step 1 through Step 6.
- To configure the BLF/SpeedDial phone feature for presence, performStep 2 and Step 5 through Step 9.

Note It is not necessary to configure presence groups or the Default Inter-Presence Group Subscription parameter for BLF/SpeedDials.

- To configure both features, perform all the steps in the checklist.

Table 20-2 Presence Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Enable the BLF for Call Lists enterprise parameter.	Configuring Presence Service Parameters and Enterprise Parameters, page 20-12
Step 2	Configure the clusterwide service parameters for presence in Cisco CallManager Administration.	Configuring Presence Service Parameters and Enterprise Parameters, page 20-12

Table 20-2 Presence Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 3	To use presence group authorization, configure presence groups and permissions.	• Understanding Presence Groups, page 20-4 • Finding Presence Groups, page 20-14 • Configuring Presence Groups, page 20-15 • Presence Group Configuration Settings, page 20-15 • Presence Group and Presence Authorization Tips, page 20-18
Step 4	Apply a presence group to the directory number, SIP trunk, SIP phone, SCCP phone, end user, and application user (for application users that are sending presence requests over the SIP trunk) in Cisco CallManager Administration. If the phone supports extension mobility and uses an autogenerated logout profile, update the autogenerated profile for the presence group.	• Understanding Presence Groups, page 20-4 • Applying a Presence Group, page 20-17 • Presence Group and Presence Authorization Tips, page 20-18 • Understanding How Presence Works with Extension Mobility, page 20-9
Step 5	To allow presence requests from a SIP trunk, check the Accept Presence Subscription check box in the SIP Trunk Security Profile Configuration window. To enable application-level authorization for a SIP trunk application in addition to trunk-level authorization, check the following check boxes in the SIP Trunk Security Profile Configuration window: • Enable Digest Authentication • Enable Application Level Authorization **Note** You cannot check Enable Application Level Authorization unless Enable Digest Authentication is checked. Apply the profile to the trunk. Reset the trunk for the changes to take effect. If you checked Enable Application Level Authorization, check the Accept Presence Subscription check box in the Application User Configuration window for the application.	• Understanding Presence Authorization, page 20-7 • Presence Group and Presence Authorization Tips, page 20-18 • "Configuring the SIP Trunk Security Profile" in the *Cisco CallManager Security Guide* • Application User Configuration, *Cisco CallManager Administration Guide*

Table 20-2 Presence Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 6	Configure the SUBSCRIBE Calling Search Space and apply the calling search space to the phone, trunk, or end user, if required. If the phone supports extension mobility and uses an autogenerated logout profile, update the autogenerated profile for the SUBSCRIBE Calling Search Space, if required.	• Understanding How the SUBSCRIBE Calling Search Space Works, page 20-8 • Configuring and Applying the SUBSCRIBE Calling Search Space, page 20-13 • Calling Search Space Configuration, *Cisco CallManager Administration Guide* • Understanding How Presence Works with Route Lists, page 20-4
Step 7	Customize phone button templates for the BLF/SpeedDial buttons.	Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons, page 20-18
Step 8	If you have not already done so, configure the phone where you want to add the BLF/SpeedDial buttons; make sure that you choose the phone button template that you configured for the BLF/SpeedDial lines.	Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
Step 9	Configure BLF/SpeedDial buttons for the phone, user device profile, or autogenerated device profile (for phones that support extension mobility).	• Introducing Presence, page 20-2 • Understanding How Presence Works with Phones and Trunks, page 20-2 • Configuring BLF/SpeedDial Buttons, page 20-19 • BLF/SpeedDial Configuration Settings, page 20-20

Configuring Presence Service Parameters and Enterprise Parameters

To configure presence enterprise parameters, for example, the BLF for Call List parameter, in Cisco CallManager Administration, choose **System > Enterprise Parameters**. For information on the parameter, click the question mark that displays in the Enterprise Parameter Configuration window or click the link for the parameter name.

To configure presence service parameters, for example, the Default Inter-Presence Group Subscription parameter, perform the following procedure:

Tip The Default Inter-Presence Group Subscription parameter does not apply to BLF/SpeedDials.

Procedure

Step 1 In Cisco CallManager Administration, choose **System > Service Parameters**.

Step 2 From the Server drop-down list box, choose the server where you want to configure the parameter.

Step 3 From the Service drop-down list box, choose the Cisco CallManager (Active) service.

If the service does not display as active, ensure that the service is activated in Cisco CallManager Serviceability.

Step 4 Locate the clusterwide service parameters for the Presence feature.

Tip For information on the parameters, click the parameter name or click the question mark that displays in the Service Parameter Configuration window.

Step 5 Update the parameter values.

Step 6 Click **Save**.

Additional Information

See the "Related Topics" section on page 20-21.

Configuring and Applying the SUBSCRIBE Calling Search Space

All calling search spaces that you configure in Cisco CallManager Administration display in the SUBSCRIBE Calling Search Space drop-down list box in the Trunk Configuration or Phone Configuration window.

The SUBSCRIBE Calling Search Space determines how Cisco CallManager routes presence requests that come from the trunk or the phone. If you do not select a different calling search space for presence requests, the SUBSCRIBE Calling Search Space defaults to None.

To configure a calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces (**Call Routing > Class of Control > Calling Search Space**). For information on how to configure a calling search space, refer to the "Calling Search Space Configuration"chapter in the *Cisco CallManager Administration Guide*.

To apply a SUBSCRIBE Calling Search Space to the SIP trunk, phone, end user, or autogenerated device profile (for phones with extension mobility support), perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- Find a phone, as described in the "Cisco IP Phone Configuration" chapter in the *Cisco CallManager Administration Guide*.
- Find a SIP trunk, as described in the "Trunk Configuration" chapter in the *Cisco CallManager Administration Guide*.
- Find an end user, as described in the "End User Configuration" chapter in the *Cisco CallManager Administration Guide*.
- Find an autogenerated device profile, as described in the "Device Profile Configuration" chapter in the *Cisco CallManager Administration Guide*.

Step 2 After the configuration window displays, choose the calling search space from the SUBSCRIBE Calling Search Space drop-down list box.

Step 3 Click **Save**.

Step 4 Click **Reset**.

Additional Information

See the “Related Topics” section on page 20-21.

Finding Presence Groups

To find a presence group, perform the following procedure:

Procedure

Step 1 In Cisco CallManager Administration, choose **System > Presence Group**.

The Find and List window displays.

Step 2 From the drop-down list boxes, choose your search criteria for the presence groups that you want to list and click **Find**.

Note To find all presence groups that exist in the database, click **Find** without specifying any search criteria.

The window refreshes and displays the presence groups that match your search criteria.

Step 3 Click the **Name** link for the presence group that you want to view.

Tip To search for the Name or Description within the search results, check the Search Within Results check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Information

See the “Related Topics” section on page 20-21.

Configuring Presence Groups

To add, update, or copy presence groups, perform the following procedure:

Procedure

Step 1 In Cisco CallManager Administration, choose **System > Presence Group**.

Step 2 Perform one of the following tasks:

- To add a new presence group, click the **Add New** button and continue with Step 3.
- To copy an existing presence group, locate the appropriate group as described in "Finding Presence Groups" section on page 20-14, click the **Copy** button next to the presence group that you want to copy, and continue with Step 3.
- To update an existing presence group, locate the appropriate group as described in "Finding Presence Groups" section on page 20-14 and continue with Step 3.
- To rename a presence group, locate the group as described in "Finding Presence Groups" section on page 20-14, click the Name link for group on the list, enter the new name when the window displays, and continue with Step 4.

Step 3 Enter the appropriate settings as described in Table 20-3.

Step 4 Click **Save**.

Additional Steps

After you configure the presence groups, apply the presence group configuration to the SIP or SCCP phone, SIP trunk, directory number, application user (for application users sending presence requests over the SIP trunk), end user, or autogenerated device profile (for phones with extension mobility support) in Cisco CallManager Administration. See the "Applying a Presence Group" section on page 20-17.

Additional Information

See the "Related Topics" section on page 20-21.

Presence Group Configuration Settings

Table 20-3 describes the presence group configuration settings. For related procedures, see the "Related Topics" section on page 20-21.

Table 20-3 Presence Group Configuration Settings

Field	Description
Name	Enter the name of the presence group that you want to configure; for example, Executive_Group.
Description	Enter a description for the presence group that you are configuring.
Modify Relationship to Other Presence Groups	Select one or more presence groups to configure the permission settings for the named group to the selected group(s).

Table 20-3 Presence Group Configuration Settings (continued)

Field	Description
Subscription Permission	For the selected presence group(s), choose one of the following options from the drop-down list box: • **Use System Default**—Set the permissions setting to the Default Inter-Presence Group Subscription clusterwide service parameter setting (Allow Subscription or Disallow Subscription). • **Allow Subscription**—Allow members in the named group to view the real-time status of members in the selected group(s). • **Disallow Subscription**—Block members in the named group from viewing the real-time status of members in the selected group(s). The permissions that you configure display in the Presence Group relationship pane when you click **Save**. All groups that use system default permission setting do not display.

Deleting a Presence Group

This section describes how to delete a presence group from the Cisco CallManager database.

Before You Begin

Before you can delete a presence group from Cisco CallManager Administration, you must apply another group to the devices/user or delete all devices/users that use the presence group.

To find out which devices/users use the presence group, click the Name link for the presence group in the Find and List window; then, choose **Dependency Records** from the Related Links drop-down list box when the Presence Group Configuration window displays; click **Go**.

If the dependency records feature is not enabled for the system, enable dependency records in the System > Enterprise Parameters window. For more information about dependency records, refer to the *Cisco CallManager System Guide*.

Procedure

Step 1 Find the presence group by using the procedure in the "Finding Presence Groups" section on page 20-14.

Step 2 To delete multiple presence groups, check the check boxes next to the appropriate check box in the Find and List window; then, click the **Delete Selected** icon or the **Delete Selected** button.

Step 3 To delete a single presence group, perform one of the following tasks:

- In the Find and List window, check the check box next to the appropriate presence group; then, click the **Delete Selected** icon or the **Delete Selected** button.
- In the Find and List window, click the Name link for the presence group. After the specific Security Profile Configuration window displays, click the **Delete Selected** icon or the **Delete Selected** button.

Step 4 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Additional Information

See the "Related Topics" section on page 20-21.

Applying a Presence Group

For information on configuring presence groups in Cisco CallManager Administration, see the "Understanding Presence Groups" section on page 20-4. For information about configuring permission settings for presence authorization, see the "Understanding Presence Authorization" section on page 20-7. The system always allows presence requests between members in the same presence group.

To apply a presence group to the directory number, SIP trunk, SIP phone, SCCP phone, application user (for application users that are sending presence requests over the SIP trunk), end user, or autogenerated device profile (for phones with extension mobility support only), perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- Find a SIP trunk, as described in the "Trunk Configuration" chapter in the *Cisco CallManager Administration Guide*.
- Find an application user, as described in the "Application User Configuration" chapter in the *Cisco CallManager Administration Guide*.
- Find an end user, as described in the "End User Configuration" chapter in the *Cisco CallManager Administration Guide*.
- Find an autogenerated device profile (phones with extension mobility support only), as described in the "Device Profile Configuration" chapter in the *Cisco CallManager Administration Guide*.
- Find a SIP or SCCP phone, as described in the "Cisco IP Phone Configuration" chapter in the *Cisco CallManager Administration Guide*.

Tip After the Phone Configuration window displays, you can access the Directory Number Configuration window by clicking the Line link in the Association Information pane. In the Directory Number Configuration window, you specify the presence group for the directory number.

When an administrator decides to add or change a BLF/SpeedDial button, the administrator ensures that the watcher is authorized to monitor that destination.

Step 2 After the configuration page displays, choose the group from the Presence Group drop-down list box. Refer to "Presence Group and Presence Authorization Tips" section on page 20-18 for provisioning tips.

Step 3 Click **Save**.

Step 4 For devices, you must click **Reset**.

Step 5 Repeat the procedure for all items that are listed in Step 1.

Additional Information

See the "Related Topics" section on page 20-21.

Presence Group and Presence Authorization Tips

Presence authorization works with presence groups. This section lists tips that you can use when you are configuring presence groups for presence authorization.

- To allow a watcher to monitor a destination, make sure that the presence group that is applied to the watcher that is originating the request, including application users, has permission to monitor the group that is applied to the presence entity. End users for supported applications, for example, IPMA end users, also serve as watchers because the user requests status about a presence entity that is configured on the application.
- To allow Cisco CallManager to receive and route presence requests from the SIP trunk application, make sure that the Accept Presence Subscription check box is checked in the Application User window to authorize incoming SUBSCRIBE requests. If no presence group is applied to the application user, Cisco CallManager uses the presence group that is applied to the trunk.
- If you check the Accept Presence Subscription check box for an application user, but do not check the Accept Presence Subscription check box in the SIP Trunk Security Profile that is applied to the trunk, a 403 error message gets sent to the SIP user agent that is connected to the trunk.
- If you check the Accept Presence Subscription check box for an application user, but do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile that is applied to the trunk, a 403 error message gets sent to the SIP user agent that is connected to the trunk.
- If digest authentication is not configured for the SIP trunk, you can configure the trunk to accept incoming subscriptions, but application-level authorization cannot be initiated, and Cisco CallManager will accept all incoming requests before performing group authorization.
- If the SIP trunk uses digest authentication, as configured in the SIP Trunk Security Profile, incoming presence requests require authentication of the credentials from the sending device. When digest authentication is used with application-level authorization, Cisco CallManager also authenticates the credentials of the application that is sending the presence requests.
- After authorization and authentication is successful for a SIP trunk application, Cisco CallManager performs group authorization to verify the group permissions that are associated with the SUBSCRIBE request before accepting the request.
- When an administrator decides to add or change a BLF/SpeedDial button for a SIP URI, the administrator ensures that the watcher is authorized to monitor that destination. If the system uses a SIP trunk to reach a SIP URI BLF target, the presence group associated with the SIP trunk applies.
- When configuring a SIP URI as BLF/SpeedDial button, make sure the routing patterns are appropriately configured. Refer to SIP Route Pattern Configuration in the *Cisco CallManager Administration Guide* for more information.

Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons

Administrators can configure BLF/SpeedDial buttons for a phone, user device profile, or autogenerated device profile. The Add a new BLF SD link does not display in the Association Information pane unless you configure a customized phone button template for BLF/SpeedDial buttons and apply the template to the phone or user device profile. After you apply the template to the phone or device profile (and save the phone or device profile configuration), the Add a new BLF SD link displays in the Association Information pane.

Tip If the template does not support BLF/SpeedDials, the Add a new BLF SD link displays in the Unassigned Associated Items pane.

To configure a customized phone button template for BLF/SpeedDial buttons, perform the following procedure:

Procedure

Step 1 Find the phone button template for the device, as described in the "Phone Button Template Configuration" chapter in the *Cisco CallManager Administration Guide*.

Step 2 After the Find/List window displays, click the **Copy** button for the phone button template.

Step 3 In the Button Template Name field, enter a new name for the template; for example, BLF SIP 7970.

Step 4 Click **Save**.

Step 5 After the Phone Button Template Configuration window displays, choose Speed Dial BLF from the Feature drop-down list box(es); that is, if you want the line to be configured as a BLF/SpeedDial button.

Step 6 Click **Save**.

Step 7 If you are updating an existing customized phone button template that you already applied to phones, click **Reset**.

Configuring BLF/SpeedDial Buttons

To configure BLF/SpeedDial buttons, perform the following procedure:

Procedure

Step 1 To configure the BLF/SpeedDial button in the Phone Configuration window, find a phone, as described in the "Cisco IP Phone Configuration" chapter in the *Cisco CallManager Administration Guide*.

Step 2 To configure the BLF/SpeedDial button for user or autogenerated device profiles, find the user device profile or autogenerated device profile (for phones with extension mobility support), as described in the "Device Profile Configuration" chapter in the *Cisco CallManager Administration Guide*.

Step 3 After the configuration window displays, click the Add a New BLF SD link in the Associated Information pane.

Tip The link does not display in the Associated Information pane if the phone button template that you applied to the phone or device profile does not support BLF/SpeedDials. The link displays in the Unassigned Associated Items pane if the phone button template does not support BLF/SpeedDials.

Step 4 Configure the settings, as described in Table 20-4. Administrators must ensure that the watcher is authorized to monitor a destination that is configured as a BLF/SpeedDial button.

Step 5 After you complete the configuration, click **Save** and close the window.

The destination(s) and/or directory number(s) display in the pane.

Additional Information

See the "Related Topics" section on page 20-21.

BLF/SpeedDial Configuration Settings

Table 20-4 describes the settings that you configure for BLF/SpeedDial buttons.

Table 20-4 BLF/SpeedDial Button Configuration Settings

Field	Description
Destination	Perform one of the following tasks to configure a SIP URI or a directory number as a BLF/SpeedDial button: • For SIP phones only, enter the SIP URI. For SCCP phones, you cannot configure SIP URI as BLF/SpeedDial buttons. • For SIP or SCCP phones, enter a directory number in this field or go to the Directory Number drop-down list box. If you want to configure nonCisco CallManager directory numbers as BLF/SpeedDial buttons, enter the directory number in this field. For this field, enter only numerals, asterisks (*), and pound signs (#). If you configure the Destination field, do not choose an option from the Directory Number drop-down list box. If you choose an option from the Directory Number drop-down list box after you configure the Destination, Cisco CallManager deletes the Destination configuration.
Directory Number	The Directory Number drop-down list box displays a list of directory numbers that exist in the Cisco CallManager database. Configure this setting only if you did not configure the Destination field. For SCCP or SIP phones, choose the number (and corresponding partition, if it displays) that you want the system to dial when the user presses the speed-dial button; for example, 6002-Partition 3. Directory numbers that display without specific partitions belong to the default partition.
Label	Enter the text that you want to display for the BLF/SpeedDial button. This field supports internationalization. If your phone does not support internationalization, the system uses the text that displays in the Label ASCII field.

Table 20-4 BLF/SpeedDial Button Configuration Settings (continued)

Field	Description
Label ASCII	Enter the text that you want to display for the speed-dial button. The ASCII label represents the noninternationalized version of the text that you enter in the Label field. If the phone does not support internationalization, the system uses the text that displays in this field. **Tip** If you enter text in the Label ASCII field that differs from the text in the Label field, Cisco CallManager Administration accepts the configuration for both fields, even though the text differs.

Where to Find More Information

Related Topics

- Introducing Presence, page 20-2
- Understanding How Presence Works with Phones and Trunks, page 20-2
- Understanding How Presence Works with Route Lists, page 20-4
- Understanding Presence Groups, page 20-4
- Understanding Presence Authorization, page 20-7
- Understanding How the SUBSCRIBE Calling Search Space Works, page 20-8
- Presence Feature Interactions/Restrictions, page 20-9
- Presence Configuration Checklist, page 20-10
- Configuring Presence Service Parameters and Enterprise Parameters, page 20-12
- Configuring and Applying the SUBSCRIBE Calling Search Space, page 20-13
- Finding Presence Groups, page 20-14
- Configuring Presence Groups, page 20-15
- Presence Group Configuration Settings, page 20-15
- Deleting a Presence Group, page 20-16
- Applying a Presence Group, page 20-17
- Presence Group and Presence Authorization Tips, page 20-18
- Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons, page 20-18
- Configuring BLF/SpeedDial Buttons, page 20-19
- BLF/SpeedDial Configuration Settings, page 20-20

Additional Documentation

- Digest Authentication, *Cisco CallManager Security Guide*
- Authorization, *Cisco CallManager Security Guide*
- Phone administration documentation that supports your phone model and this version of Cisco CallManager

- Cisco IP Phone or Cisco SIP IP Phone user documentation
- Firmware release notes for your phone model

INDEX

A

- AAR
  - MLPP interaction 13-26
- access
  - restricting with partitions 10-3
- access control
  - MLPP numbering plan
    - example (figure) 13-20
    - explained 13-19
  - precedence patterns
    - example (figure) 13-20
    - explained 13-19
- ac user
  - associating with devices and pilot points 16-27
  - configuring 16-20
- alternate party diversion (APD)
  - example (figure) 13-9
  - explained 13-9
- announcements
  - blocked precedence 13-18
  - blocked precedence (figure) 13-18
  - busy station 13-18
  - MLPP 13-16
  - unauthorized precedence 13-17
  - unauthorized precedence (figure) 13-17
- application dial rules
  - configuring for WebDialer 15-10
- Attendant Console, Cisco CallManager
  - associating devices and pilot points with the ac user 16-27
  - client configuration settings (table) 16-35
  - configuration checklist 16-16
  - configuring 16-15
  - configuring attendant settings 16-35
  - configuring held icon timers 16-37
  - CorporateDirectory.txt file
    - creating and uploading 16-31
    - deleting 16-33
  - dependency records 16-38
  - directory 16-9
  - hunt groups
    - configuration settings (table) 16-29
    - deleting members 16-30
    - understanding 16-2
    - viewing members 16-30
  - installation and activation 16-15
  - installing 16-33
  - interactions 16-13
  - overview 16-1
  - performance monitors 16-38
  - pilot points
    - configuration settings 16-24
    - configuring 16-23
    - deleting 16-26
    - finding 16-22
    - resetting 16-26
    - understanding 16-2
  - redundancy 16-11
  - restrictions 16-14
  - service parameters 16-31
  - starting after installing Windows XP SP2 16-34
  - system requirements 16-12
  - users
    - configuration settings 16-19
    - configuring 16-17

configuring the ac user 16-20
deleting 16-20
finding 16-17
understanding 16-2
audio sources
configuring 6-16
creating for MOH 6-9
default MOH sample 6-9
for MOH 6-8
managing for MOH 6-10
multicast 6-10
storing for MOH 6-9
unicast 6-10
auto call pickup 10-2
automated alternate routing (AAR)
MLPP interaction 13-26

B

bandwidth
insufficient with AAR for MLPP 13-26
barge
activating with built-in conference bridge 8-8
configuration checklist (table) 8-9
installing and activating 8-8
interactions and restrictions 8-6
overview 8-1
service parameters 8-10
softkey 8-3
system requirements 8-5
BLF/SpeedDial
buttons 20-19
configuration settings (table) 20-20
configuring 20-18
built-in conference bridge
barge 8-8

C

call display restrictions
configuration checklist (table) 17-5
configuring 17-5
configuring in user device profile 1-19
enabling 17-2
interactions 17-3
introduction 17-1
overview 17-1
sample configurations 17-8
scenarios 17-3
system requirements 17-3
call forward
MLPP interaction 13-24
calling search spaces
Cisco IP Manager Assistant (IPMA)
configuration tips 2-16
SUBSCRIBE (for Presence) 20-8, 20-13
call park
configuration checklist (table) 9-6
configuration settings (table) 9-10
configuring 9-6
configuring a number 9-9
deleting a number 9-11
example with MOH 6-5
finding a number 9-7
installing and activating 9-6
interactions 9-4
introduction 9-1
overview 9-1
restrictions 9-6
setting service parameters 9-7
system requirements 9-4
troubleshooting 9-11
usage example 9-2
call pickup group
assigning call pickup group to a directory number 10-14
auto call pickup 10-2

configuration checklist (table) 10-6
configuration settings (table) 10-12
configuring 10-1, 10-11
defining a pickup group for other group call pickup 10-13
deleting 10-13
finding 10-10
installing and activating 10-1
interactions and restrictions 10-4
introducing 10-1
restricting access 10-3
setting the service parameters 10-9
system requirements 10-1, 10-3
using with partitions 10-3

call preservation
with MLPP 13-26

call queuing 16-9

call transfer
MLPP interaction 13-25

call waiting
MLPP interaction 13-25

cBarge
activating with shared conference bridge 8-8
softkey 8-4

CDR
recording for precedence calls 13-24

channel nonpreemptable 13-12

Cisco Call Back
additional information for Cisco Call Back notification with SIP phones 4-5
configuration checklist 4-7
description 4-1
interactions and restrictions 4-5
interactions with Call Forward, iDivert, and Voice-Mail System features 4-6
overview 4-1
setting service parameters 4-9
softkey template 4-7
suspend/resume functionality 4-4
system requirements 4-4
understanding 4-2

Cisco CallManager
configuring for Cisco CallManager AutoAttendant 7-5
MOH servers 6-6

Cisco CallManager Attendant Console
associating devices and pilot points with ac user 16-27
client configuration settings (table) 16-35
configuration checklist 16-16
configuring 16-15
configuring attendant settings 16-35
configuring held icon timers 16-37
CorporateDirectory.txt file
creating and uploading 16-31
deleting 16-33
dependency records 16-38
directory 16-9
hunt groups
configuration settings (table) 16-29
deleting members 16-30
understanding 16-2
viewing members 16-30
installation and activation 16-15
installing 16-33
interactions 16-13
overview 16-1
performance monitors 16-38
pilot points
configuration settings 16-24
configuring 16-23
deleting 16-26
finding 16-22
resetting 16-26
understanding 16-2
redundancy 16-11
restrictions 16-14
Server 16-10
service parameters 16-31
starting after installing Windows XP SP2 16-34
system requirements 16-12

users
  configuration settings 16-19
  configuring 16-17
  configuring the ac user 16-20
  deleting 16-20
  finding 16-17
  understanding 16-2
Cisco CallManager AutoAttendant 7-5
  adding a JTAPI call control group 7-11
  adding to Cisco CRS 7-16, 7-17
  CCM AA and the CRS engine 7-4
  choose media types 7-15
  cluster setup 7-10
  components 7-3
  configuration (table) 7-5
  configuring welcome prompt 7-22
  customizing 7-20
  description 7-1
  installation requirements 7-3
  installing 7-4
  installing or upgrading 7-4
  installing the CRS engine 7-3
  managing 7-24
  modifying instance 7-20
  modifying prompts 7-21
  overview 7-2
  provisioning Cisco media termination subsystem 7-15
  recording welcome prompt 7-21
  script 7-2
  server setup 7-11
  understanding 7-1
  uploading spoken name 7-23
Cisco CallManager Extension Mobility
  adding 1-15
  configuration checklist 1-13
  configuration checklist (table) 7-5
  configuration example 1-12
  configuring 1-11
  description 1-3
  device profiles 1-2
  illustrated (figure) 1-4
  installing 1-10
  interaction with Presence 20-9
  login call flow 1-6
  logout call flow 1-7
  overview 1-1
  subscribing 1-24
  system requirements 1-7
  user device profile, associating 1-23
  using 1-26
Cisco CRS engine 7-9
  adding Cisco CallManager AutoAttendant 7-16, 7-17
  configuring for Cisco CallManager AutoAttendant 7-9
  starting and stopping 7-24
  viewing trace settings 7-24
Cisco Customer Response Platform
  components 7-3
Cisco IP Manager Assistant (IPMA)
  architecture overview 2-2, 3-2
  assistant console dialog options 2-32, 3-22
  assistant console interface 2-4, 3-3
  assistant interfaces 2-5, 3-4
  bulk administration tool 1-9, 2-7, 3-6
  calling search space and partitions
    configuration tips 2-16
  Cisco IP Phone interface 2-4, 3-4
  Cisco IP Phone Services, configuration tips 2-20
  configuration checklist for proxy line support (table) 2-11
  configuration checklist with shared line support (table) 3-9
  configuration wizard for proxy line 2-13
  configuring assistant phones
    tips 2-23
  configuring assistant proxy and incoming intercom lines 2-28
  configuring manager and assigning assistant for proxy line 2-25

configuring manager and assigning assistant for shared line 3-16
configuring manager phones
tips 2-22
configuring manager primary and incoming intercom lines 2-25, 3-16
configuring shared and incoming intercom lines for assistant 3-18
database and directory access architecture
understanding 2-5, 3-4
deleting assistant information 2-29, 3-20
deleting manager information 2-26, 3-17
dial rules configuration 2-31, 3-21
extension mobility 2-7, 3-6
installing and activating 2-10, 3-8
installing the assistant console application 2-32, 3-22
IPMASecureSysUser 2-20, 3-13
manager and assistant phone configuration 2-21, 3-13
manager assistant administration interface 2-6, 3-5
manager configuration 2-32, 3-23
manager interfaces 2-5, 3-4
multilevel precedence and preemption 2-9
Multilevel Precedence and Preemption (MLPP) 3-8
phones
configuration tips 2-24, 3-15
providing information to managers and assistants 2-31, 3-22
reporting tools 2-8, 3-7
restrictions 2-9, 3-8
route point
configuration tips 2-17
security 2-20, 3-13
setting service parameters 2-18, 3-11
softkeys 2-5, 3-4
starting the Cisco IPMA service 2-20, 3-13
system configuration with proxy line 2-13
system requirements 2-6, 3-5
time-of-day routing 2-9
understanding 2-2, 3-2
updating assistant information 2-30, 3-20
updating manager information 2-27, 3-18
Cisco IP Phone Services
Cisco IP Manager Assistant (IPMA)
configuration tips 2-20
Cisco WebDialer 15-1
Client Matter Codes
configuration checklist (table) 5-5
configuration settings (table) 5-8
configuring 5-7
CTI, JTAPI, and TAPI usage 5-4
deleting 5-8
described 5-2
enabling for route patterns 5-8
finding 5-6
installation 5-5
interactions 5-3
requirements 5-5
restrictions 5-3
system requirements 5-5
user information 5-13
common network facility preemption
example (figure) 13-13
example with retry timer Trr (figure) 13-14
explained 13-12
CorporateDirectory.txt file
creating and uploading 16-31
deleting 16-33
CRS
server setup 7-11
CRS engine
hardware and software requirements 7-3
CTI route points
Cisco IP Manager Assistant (IPMA) configuration tips 2-17
Customer Response Solutions
server 7-11
Customer Response Solutions engine
installing and upgrading 7-3

custom phone rings

creating 14-3

customizing files 14-2

introduction 14-1

overview 14-1

PCM file requirements 14-3

D

database

scalability 6-7

dependency records

Cisco CallManager Attendant Console 16-38

device profiles

and Cisco CallManager Extension Mobility 1-2

directory

Cisco CallManager Attendant Console, understanding 16-9

directory number

assigning a call pickup group 10-14

directory server settings, Cisco CallManager AutoAttendant 7-10

domain

identifier for MLPP 13-6

E

enterprise parameters

MLPP 13-29

Presence 20-12

external call transfer restrictions

block offnet to offnet transfer service parameter 19-7

call classification service parameter 19-7

configuration checklist (table) 19-6

gateway configuration 19-7

installing and activating 19-5

interactions 19-5

overview 19-1

restrictions 19-5

route pattern configuration 19-8

service parameters 19-7

system requirements 19-4

trunk configuration 19-8

F

features

barge 8-1

call display restrictions 17-1

call park 9-1

Cisco IP Manager Assistant (IPMA)

assistant console interface 2-4, 3-3

assistant interfaces 2-5, 3-4

bulk administration tool 1-9, 2-7, 3-6

calling search space and partitions 2-16

Cisco IP Phone interface 2-4, 3-4

Cisco IP Phone Services 2-20

configuration checklist for proxy line support (table) 2-11

configuration checklist with shared line support (table) 3-9

extension mobility 2-7, 3-6

manager assistant administration interface 2-6, 3-5

manager interfaces 2-5, 3-4

multilevel precedence and preemption 2-9

Multilevel Precedence and Preemption (MLLP) 3-8

phones 2-24, 3-15

reporting tools 2-8, 3-7

route point 2-17

softkeys 2-5, 3-4

time-of-day routing 2-9

understanding 2-2, 3-2

understanding architecture 2-2, 3-2

understanding database and directory access architecture 2-5, 3-4

external call transfer restrictions 19-1

immediate divert 11-1

Malicious Call ID (MCID) 12-1

Multilevel Precedence and Preemption (MLPP)
using with Cisco IPMA 3-8
Presence 20-1, 20-2
privacy 8-1
QRT 18-1
WebDialer 15-1
file format
Ringlist.xml 14-2
fixed audio source
configuration settings (table) 6-23
configuring 6-21, 6-22
deleting 6-22
Forced Authorization Codes
configuration checklist (table) 5-5
configuration settings (table) 5-11
configuring 5-10
CTI, JTAPI, and TAPI usage 5-4
deleting 5-11
described 5-2
enabling for route patterns 5-12
finding 5-9
installation 5-5
interactions 5-3
requirements 5-5
restrictions 5-3
system requirements 5-5
user information 5-13

G

group call pickup
configuration settings (table) 10-12

H

held icon timers, configuring 16-37
hunt groups
broadcast, understanding 16-8
circular, understanding 16-6
configuration settings (table) 16-29
configuring 16-28
deleting members 16-30
linked, understanding 16-5
understanding 16-2
viewing members 16-30

I

immediate divert
configuration checklist (table) 11-7
installing and activating 11-7
interactions 11-5
more information 11-8
overview 11-1
restrictions 11-6
setting service parameters 11-8
system requirements 11-2
using 11-4
indication enabled 13-7
insufficient bandwidth
AAR for MLPP 13-26

L

lines
interaction with MLPP 13-24
login call flow
Cisco CallManager Extension Mobility 1-6
logout call flow
Cisco CallManager Extension Mobility 1-7

M

malicious call ID
adding a softkey template 12-6
configuration checklist (table) 12-4

configuring alarms 12-6
explained
giving MCID to users 12-7
installing 12-4
interactions 12-2
overview 12-1
removing MCID feature 12-7
restrictions 12-4
services 12-1
setting service parameters 12-5
system requirements 12-2
troubleshooting 12-8
using feature with Cisco CallManager 12-2
feature code 12-2
Malicious Call Identification (MCID), see malicious call ID
MCGP
and MLPP 13-26
MLPP
activating 13-28
announcements
blocked precedence 13-18
blocked precedence (figure) 13-18
busy station 13-18
explained 13-16
unauthorized precedence 13-17
unauthorized precedence (figure) 13-17
automated alternate routing (AAR) 13-26
call forward 13-24
call preservation 13-26
call transfer 13-25
call waiting 13-25
CDR recording 13-24
configuration checklist (table) 13-28
described 13-1
domain 13-6
enterprise parameters 13-29
hierarchical configuration 13-23
indication 13-7
installing 13-28
interactions 13-26, 13-27
introducing 13-1
line feature interaction 13-24
MGCP 13-26
numbering plan
example (figure) 13-20
explained 13-19
precedence
alternate party diversion (APD) 13-9
alternate party diversion example (figure) 13-9
call setup 13-8
explained 13-3
patterns 13-7
precedence patterns
example (figure) 13-20
explained 13-19
preemption
common network facility 13-12
common network facility example (figure) 13-13
common network facility example with retry timer Trr (figure) 13-14
details 13-11
enabled 13-10
explained 13-6
receiving 13-10
user access 13-11
user access channel nonpreemptable 13-12
user access example (figure) 13-11
PRI 13-26
restrictions 13-26, 13-27
service parameter 13-23
shared lines 13-25
terminology 13-2
trunk selection
example (figure) 13-22
explained 13-21
modifying files 14-2

MOH
- audio sources 6-16
  - configuration settings (table) 6-19
  - configuring 6-18
  - deleting 6-19
  - explained 6-8
  - finding 6-17
- call park example 6-5
- characteristics 6-3
- configuration checklist (table) 6-14
- configuring 6-23
- creating audio sources 6-9
- database scalability 6-7
- default MOH sample 6-9
- definitions 6-2
- described 6-1
- failover and fallback 6-13
- features
  - database requirements 6-6
  - database scalability 6-7
  - manageability 6-7
  - MOH servers 6-5
  - server manageability 6-6
  - server redundancy 6-6
  - server scalability 6-6
- fixed audio source 6-21
  - configuration settings (table) 6-23
  - configuring 6-22
  - deleting 6-22
- functionality 6-4
- list of topics 6-1
- managing audio sources 6-10
- monitoring performance
  - overview (table) 6-15
  - service states 6-16
- requirements and limits 6-12
- server configuration settings (table) 6-26
- servers
  - characteristics 6-5
  - configuring 6-24
  - database requirements 6-6
  - explained 6-8
  - finding 6-23
  - manageability 6-6
  - perfmon counters 6-15
  - redundancy 6-6
  - resetting 6-25
  - scalability 6-6
- storing audio sources 6-9
- supported features 6-5
- transfer hold example 6-5
- understanding 6-1
- user hold example 6-5

multicast
- audio sources for MOH 6-10
- configuration checklist (table) 6-11
- explained 6-10

multilevel precedence and preemption
- activating 13-28
- announcements
  - blocked precedence 13-18
  - blocked precedence (figure) 13-18
  - busy station 13-18
  - explained 13-16
  - unauthorized precedence 13-17
  - unauthorized precedence (figure) 13-17
- automated alternate routing (AAR) 13-26
- call forward 13-24
- call preservation 13-26
- call transfer 13-25
- call waiting 13-25
- CDR recording 13-24
- configuration checklist (table) 13-28
- described 13-1
- domain 13-6
- enterprise parameters 13-29
- hierarchical configuration 13-23
- indication 13-7

installing 13-28
interactions 13-26, 13-27
introducing 13-1
line feature interaction 13-24
MGCP 13-26
numbering plan
example (figure) 13-20
explained 13-19
precedence
alternate party diversion (APD) 13-9
alternate party diversion example (figure) 13-9
call setup 13-8
explained 13-3
patterns 13-7
precedence patterns
example (figure) 13-20
explained 13-19
preemption
common network facility 13-12
common network facility example (figure) 13-13
common network facility example with retry timer Trr (figure) 13-14
details 13-11
enabled 13-10
explained 13-6
receiving 13-10
user access 13-11
user access channel nonpreemptable 13-12
user access example (figure) 13-11
restrictions 13-26, 13-27
service parameter 13-23
shared lines 13-25
terminology 13-2
trunk selection
example (figure) 13-22
explained 13-21
music on hold (MOH) 6-16, 6-21, 6-23
audio sources 6-8
call park example 6-5
characteristics 6-3
configuration checklist (table) 6-14
creating audio sources 6-9
default MOH sample 6-9
definitions 6-2
described 6-1
failover and fallback 6-13
functionality 6-4
list of topics 6-1
managing audio sources 6-10
monitoring performance
overview (table) 6-15
service states 6-16
requirements and limits 6-12
servers
characteristics 6-5
database requirements 6-6
explained 6-8
manageability 6-6
perfmon counters 6-15
redundancy 6-6
scalability 6-6
storing audio sources 6-9
supported features 6-5
transfer hold example 6-5
understanding 6-1
user hold example 6-5

N

nonpreemptable user access channel 13-12
numbering plan
MLPP (figure) 13-20
MLPP access control 13-19

O

other call pickup
- configuration checklist (table) 10-8

P

parameters, service
- CDR 12-5

partitions
- restricting access 10-3
- using call pickup 10-3

partition support
- overview 15-9

PCM file requirements
- for custom ring types 14-3

perfmon counters
- counter descriptions (table) 6-16
- using to view MOH servers 6-15

phones
- custom rings
  - creating 14-1, 14-3
  - overview 14-1
  - PCM file requirements 14-3
- interaction with Presence 20-2

pilot points
- associating with the ac user 16-27
- configuration settings 16-24
- configuring 16-23
- deleting 16-26
- finding 16-22
- resetting 16-26
- understanding 16-2

precedence
- alternate party diversion (APD)
  - example (figure) 13-9
  - explained 13-9
- blocked 13-18
- blocked (figure) 13-18
- busy station 13-18
- call setup 13-8
- CDR recording 13-24
- explained 13-3
- patterns
  - access control 13-19
  - MLPP (figure) 13-20
  - setup 13-7
- unauthorized 13-17
- unauthorized (figure) 13-17

preemption
- common network facility 13-12
- common network facility example (figure) 13-13
- common network facility example with retry timer Trr (figure) 13-14
- details 13-11
- enabled 13-10
- explained 13-6
- receiving 13-10
- user access 13-11
- user access channel nonpreemptable 13-12
- user access example (figure) 13-11

Presence
- authorization 20-7
- BLF/SpeedDial
  - configuration settings (table) 20-20
  - configuring 20-18
- BLF/SpeedDial buttons
  - configuring 20-19
- configuration checklist (table) 20-10
- feature interactions and restrictions 20-9
- groups 20-4
  - applying 20-17
  - configuration example 20-5
  - configuration settings (table) 20-15
  - interaction examples 20-6, 20-7
- interaction with Extension Mobility 20-9
- interaction with phones and trunks 20-2
- interaction with route lists 20-4

more information 20-21
overview 20-1, 20-2
request
examples 20-3
SUBSCRIBE calling search space 20-8, 20-13
tips for presence group and presence authorization 20-18
PRI
and MLPP 13-26
privacy
activating 8-8
configuration checklist (table) 8-10
installing and activating 8-8
interactions and restrictions 8-6
overview 8-1
service parameters 8-10
system requirements 8-5
prompts, Cisco CallManager AutoAttendant 7-21
proxy user
creating for WebDialer 15-11

Q

QRT
adding softkey template to phones 18-20
Cisco Extended Functions service 18-5
configuration checklist 18-16
configuring 18-15
creating softkey template 18-16
description 18-1
extended menu choices 18-9
installing 18-14
interactions and restrictions 18-14
IP phone support 18-5
overview 18-1
problem categories and reason codes 18-10
QRT reports 18-26
securing signaling connections 18-7
serviceability features 18-21
setting service parameters 18-24
system requirements 18-5
user interface 18-8
using 18-8
using the QRT Viewer 18-26
Quality Report Tool (QRT) 18-1

R

redirector servlet
configuring 15-9
redundancy
Cisco CallManager Attendant Console 16-11
MOH servers 6-6
WebDialer 15-2
requirements
Cisco Call Back 4-4
Cisco CallManager Extension Mobility 1-7
retry timer Trr example (figure) 13-14
Ringlist.xml file format 14-2
route list
interaction with Presence 20-4

S

security
Cisco IPMA 2-20, 3-13
IPMASecureSysUser 2-20, 3-13
Presence authorization 20-7
service parameters
barge 8-10
CDR 12-5
external call transfer restrictions 19-7
MLPP 13-23
Presence 20-12
privacy 8-10
WebDialer 15-6

services
- Cisco CallManager Extension Mobility, adding 1-15

shared conference bridge
- cBarge 8-8

shared lines
- MLPP interaction 13-25

softkey
- barge 8-3
- cBarge 8-4
- templates for MCID 12-6

spoken name, uploading 7-23

standard CCM end users group
- adding users for WebDialer 15-10

T

templates, softkey
- MCID 12-6

trace settings
- WebDialer 15-12

transfer
- external call transfer restrictions 19-1

transfer hold, example with MOH 6-5

Trr retry timer preemption example (figure) 13-14

trunks
- interaction with Presence 20-2
- selection for MLPP
  - example (figure) 13-22
  - explained 13-21

U

unicast
- audio sources for MOH 6-10
- explained 6-10

user hold, example with MOH 6-5

users
- Cisco CallManager Attendant Console
  - configuring 16-17
  - understanding 16-2

W

WebDialer
- adding users to standard CCM end users group 15-10
- configuration checklist (table) 15-5
- configuring application dial rules 15-10
- configuring Webdialer servlet 15-6
- creating a proxy user 15-11
- installing and activating 15-4
- interactions and restrictions 15-3
- overview 15-1
- redirector servlet 15-2
- redundancy 15-2
- service parameters 15-6
- servlet
  - configuring 15-6
  - described 15-1
- system requirements 15-3
- trace settings 15-12