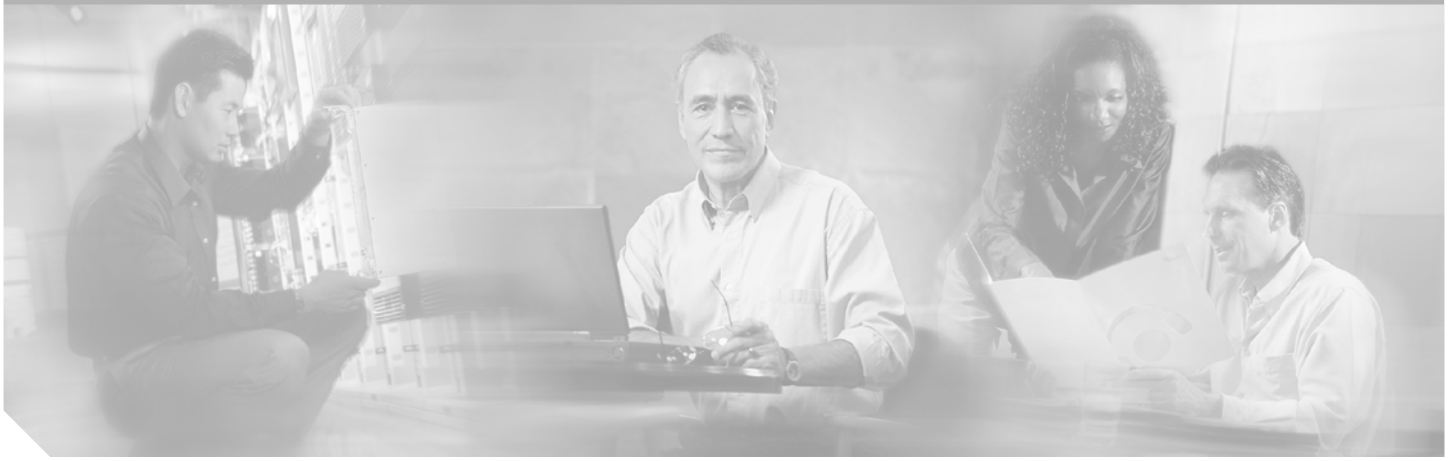


Cisco Unified CallManager System Guide

Release 5.0(4)

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-10048-01

Cisco Unified CallManager System Guide

CONTENTS

Preface xxiii

Purpose xxiii

Audience xxiv

Organization xxiv

Related Documentation xxv

Conventions xxv

Obtaining Documentation xxvi

Cisco.com xxvi

Product Documentation DVD xxvii

Ordering Documentation xxvii

Documentation Feedback xxvii

Cisco Product Security Overview xxvii

Reporting Security Problems in Cisco Products xxviii

Obtaining Technical Assistance xxix

Cisco Technical Support & Documentation Website xxix

Submitting a Service Request xxix

Definitions of Service Request Severity xxx

Obtaining Additional Publications and Information xxx

PART 1 Understanding Cisco Unified CallManager

CHAPTER 1 Introduction 1-1

Cisco Unified CallManager as an Appliance 1-1

Key Features and Benefits 1-2

Where to Find More Information 1-3

CHAPTER 2 Cisco Unified Communications Overview 2-1

Internet Ecosystem 2-1

Cisco Unified Communications Support 2-1

Applications 2-2

Call Processing 2-2

Infrastructure 2-3

Clients 2-3

Cisco Unified Communications Network 2-3

Where to Find More Information 2-4

PART 2 Understanding Cisco Unified CallManager System Configuration

CHAPTER 3 System Configuration Overview 3-1

Basic Configuration Flow 3-1

Where to Find More Information 3-4

CHAPTER 4 Roles and User Groups 4-1

Overview 4-1

Roles 4-2

Role Access Privileges 4-2

User Groups 4-3

Access Log 4-3

Enterprise Parameters 4-3

Standard Roles and User Groups 4-4

Where to Find More Information 4-4

CHAPTER 5 System-Level Configuration Settings 5-1

Server Configuration 5-1

Cisco Unified CallManager Configuration 5-2

Cisco Unified CallManager Groups 5-3

Phone NTP Reference Configuration for SIP Phones 5-4

Date/Time Groups 5-4

Regions 5-5

Device Pools 5-10

Updating Device Pools 5-11

LDAP 5-12

Call Admission Control 5-13

Survivable Remote Site Telephony References 5-13

MLPP Domain 5-15

Enterprise Parameters 5-15

Service Parameters 5-16

Dependency Records 5-16

System Configuration Checklist 5-17

Where to Find More Information 5-18

CHAPTER 6 Clustering 6-1

Clusters 6-1

Intercluster Communication 6-2

Balanced Call Processing 6-3

Where to Find More Information 6-4

CHAPTER 7 Redundancy 7-1

Cisco Unified CallManager Redundancy Groups 7-1

Cisco Unified CallManager Groups 7-1

Distributing Devices for Redundancy and Load Balancing 7-3

Media Resource Redundancy 7-4

CTI Redundancy 7-4

Where to Find More Information 7-4

CHAPTER 8 Call Admission Control 8-1

Locations 8-2

Locations and Regions 8-3

Bandwidth Calculations 8-4

Location-Based MLPP 8-5

Locations Configuration Checklist 8-6

Gatekeepers and Trunks 8-6

Components of Gatekeeper Call Admission Control 8-8

Gatekeeper and Trunk Configuration on the Router 8-8

Gatekeeper and Trunk Configuration in Cisco Unified CallManager 8-9

Gatekeeper and Trunk Configuration Checklist 8-10

Where to Find More Information 8-10

CHAPTER 9 Resource Reservation Protocol 9-1

RSVP Overview 9-1

Advantages of RSVP 9-2

RSVP Capabilities 9-2

RSVP-Based MLPP 9-3

Additional Features 9-3

RSVP Caveats 9-4

RSVP Agent and Quality of Service 9-5

RSVP Agent Allocation 9-6

RSVP Agent Interaction with Location-Based CAC 9-6

RSVP Configuration 9-6

Clusterwide Default RSVP Policy 9-7

Location-Pair RSVP Policy 9-7

RSVP Retry 9-8

Mid-call RSVP Error Handling 9-8

MLPP-to-RSVP Priority Mapping 9-9

TSpec 9-9

Audio TSpec 9-10

Video TSpec 9-10

DSCP 9-11

Application ID 9-11

RSVP for Media Devices 9-11

Enabling RSVP for a Call 9-11

Special Configuration With RSVP 9-12

RSVP Configuration Checklist 9-12

Migrating to RSVP 9-13

Example RSVP Interactions 9-15

RSVP and Shared-Line Calls 9-15

RSVP and Music On Hold 9-16

RSVP and Call Transfer 9-18

RSVP and MLPP 9-20

Troubleshooting RSVP 9-21

Performance Monitoring Counters 9-21

Call Detail Records 9-21

Alarms 9-22

Trace Information 9-22

Where to Find More Information 9-23

CHAPTER 10 Cisco TFTP 10-1

TFTP Process Overview for SCCP Devices 10-2

TFTP Process Overview for Cisco SIP IP Phones 10-3

Understanding How Devices Use DHCP and Cisco TFTP 10-4

Understanding How Devices Access the TFTP Server 10-6

Understanding How Devices Identify the TFTP Server 10-6

Configuring a Backup or Fallback TFTP Server 10-7

Centralized TFTP in a Multiple Cluster Environment 10-7
Alternate TFTP Paths 10-8
Configuration Tips for Centralized TFTP 10-9
Customizing and Modifying Configuration Files 10-9
TFTP Configuration Checklist 10-10
Where to Find More Information 10-10

CHAPTER 11 Device Support 11-1
Supported Devices 11-1
Device Configuration Files 11-2
Device Firmware Loads 11-2
Updating Device Loads 11-3
Device Pools 11-3
Call Preservation 11-4
Call Preservation Scenarios 11-5
Where to Find More Information 11-6

CHAPTER 12 Autoregistration 12-1
Understanding Autoregistration 12-1
Autoregistration with Multiple Protocol Support 12-2
Autoregistration Configuration Checklist 12-3
Where to Find More Information 12-4

CHAPTER 13 Dynamic Host Configuration Protocol 13-1
DHCP Server 13-1
Domain Name System 13-2
DHCP Server Configuration Process 13-3
Understanding How Devices Identify the TFTP Server 13-3
Migration 13-4
Alarms 13-4
Related Topics 13-4

CHAPTER 14 Licensing 14-1
Starting License Manager Service 14-1
Splitting Licenses 14-2
Alarms 14-3

Migrating from Cisco Unified CallManager 4.0(x) to 5.0(x) 14-3
Transferring License Files 14-4
Related Topics 14-4

PART 3 Dial Plan Architecture

CHAPTER 15 Partitions and Calling Search Spaces 15-1
Understanding Partitions and Calling Search Spaces 15-1
Examples 15-2
Guidelines and Tips 15-3
Dependency Records 15-3
Partition Name Limitations 15-4
Where to Find More Information 15-4

CHAPTER 16 Time-of-Day Routing 16-1
Understanding Time-of-Day Routing 16-1
Time Periods 16-1
Time Schedules 16-2
End-Users and Time-of-Day Routing 16-2
Dependency Records 16-3
Where to Find More Information 16-3

CHAPTER 17 Understanding Route Plans 17-1
Automated Alternate Routing 17-1
Automated Alternate Routing Enable Service Parameter 17-3
Automated Alternate Routing and Hunt Pilots 17-3
Route Plan Overview 17-4
Route Groups and Route Lists 17-5
Route Patterns 17-6
Route Pattern Usage 17-6
Line Groups 17-8
Hunt Lists 17-9
Hunt Pilots 17-9
Call Coverage 17-10
Hunting and Call Forwarding 17-10
Example of Call Hunting 17-11
Maximum Hunt Timer 17-11

Internal and External Calls 17-11
Personal Preferences 17-11
Closest Match Routing 17-12
Using the @ Wildcard Character in Route Patterns 17-12
Static Digit Analysis 17-13
Special Characters and Settings 17-15
Wildcards and Special Characters in Route Patterns and Hunt Pilots 17-16
Discard Digits Instructions 17-18
Calling and Called Party Transformations 17-25
Calling Party Number Transformations Settings 17-25
Called Party Number Transformations Settings 17-27
Caller Identification and Restriction 17-28
Calling Party Presentation and Restriction Settings 17-28
Connected Party Presentation and Restriction Settings 17-30
Caller Identification Support with Device Control Protocols in Cisco Unified CallManager 17-32
External Route Plan Wizard 17-33
Generated Route Filters 17-34
Generated Route Groups 17-35
Generated Route Lists 17-35
Generated Route Patterns 17-36
Route Plan Report 17-37
Where to Find More Information 17-37
CHAPTER 18 Understanding Directory Numbers 18-1
Characteristics of Directory Numbers 18-1
Shared Line Appearance 18-2
Managing Directory Numbers 18-5
Directory Number Features 18-5
Making and Receiving Multiple Calls Per Directory Number 18-7
Transfer and Conference Behavior 18-7
Direct Transfer and Join Behavior 18-7
Directory Number Search 18-8
Dependency Records 18-9
Directory Number Configuration Checklist 18-9
Where to Find More Information 18-10

CHAPTER 19 **Dial Rules Overview** 19-1

Application Dial Rules Configuration Design 19-1

Application Dial Rules Configuration Error Checking 19-2

Directory Lookup Dial Rules 19-3

SIP Dial Rules 19-4

SIP Dial Rule Patterns 19-4

SIP Dial Rule Parameters 19-5

Private Line Automatic Ringdown (PLAR) 19-7

Where to Find More Information 19-8

PART 4 **LDAP Directory and User Configuration**

CHAPTER 20 **Understanding the Directory** 20-1

Cisco Unified CallManager and the Corporate LDAP Directory 20-2

Directory Access 20-3

DirSync Service 20-3

DirSync Service Parameters 20-4

Data Migration Assistant 20-4

Authentication 20-4

Using the Cisco Unified CallManager Database Versus the Corporate LDAP Directory 20-5

Directory Access for Cisco Unified Communications Endpoints 20-5

LDAP Directory Configuration Checklist 20-6

Where to Find More Information 20-7

CHAPTER 21 **Application Users and End Users** 21-1

How Cisco Unified CallManager JTAPI Uses the Directory 21-1

Application Users 21-2

End Users 21-2

Application Profiles 21-3

Device Association 21-3

Device Association for Application Users 21-3

Device Association for End Users 21-4

Cisco Extension Mobility Profiles 21-4

Cisco IP SoftPhone Profiles 21-5

Managing Application User and End User Configuration Checklist 21-5

Where to Find More Information 21-6

PART 5 **Media Resources**

CHAPTER 22 **Media Resource Management** 22-1

Understanding Media Resources 22-1

Media Resource Groups 22-3

Media Resource Group Lists 22-4

Dependency Records 22-6

Media Resource Group and Media Resource Group List Configuration Checklist 22-6

Where to Find More Information 22-7

CHAPTER 23 **Annunciator** 23-1

Understanding Annunciators 23-1

Planning Your Annunciator Configuration 23-2

Annunciator System Requirements and Limitations 23-3

Supported Tones and Announcements 23-4

Dependency Records 23-5

Annunciator Performance Monitoring and Troubleshooting 23-5

Annunciator Configuration Checklist 23-5

Where to Find More Information 23-6

CHAPTER 24 **Conference Bridges** 24-1

Understanding Conference Devices 24-1

- Router-Based Conference Capability 24-2
- Software Conference Devices 24-3
- Video Conference Devices 24-3
- Cisco Conference Devices (WS-SVC-CMM) 24-3
- MTP WS-X6608 DSP Service Card 24-4
- Annunciator Support for Conference Bridges 24-4
- Conference Bridge Types in Cisco Unified CallManager Administration 24-4

Using Different Conference Types: Meet Me and Ad Hoc 24-6

- Initiating an Ad Hoc Conference 24-6
  - Ad Hoc Conference Settings 24-7
  - Ad Hoc Conference Settings Restrictions for SIP Phones 24-8
  - Ad Hoc Conference Limitations 24-9
- Initiating a Meet-Me Conference 24-9
  - Meet-Me Conference Limitations 24-9

Dependency Records 24-9

Conference Bridge Performance Monitoring and Troubleshooting 24-10

Conference Bridge Configuration Checklist 24-11

Where to Find More Information 24-11

CHAPTER 25 **Transcoders** 25-1

Understanding Transcoders 25-1

Managing Transcoders with the Media Resource Manager 25-2

Using Transcoders as MTPs 25-2

Transcoder Types in Cisco Unified CallManager Administration 25-2

Transcoder Failover and Fallback 25-3

Active Cisco Unified CallManager Becomes Inactive 25-4

Resetting Registered Transcoder Devices 25-4

Dependency Records 25-4

Transcoder Performance Monitoring and Troubleshooting 25-4

Transcoder Configuration Checklist 25-5

Where to Find More Information 25-5

CHAPTER 26 **Music On Hold** 26-1

CHAPTER 27 **Media Termination Points** 27-1

Understanding Media Termination Points 27-1

SIP and MTP 27-2

Managing MTPs with the Media Resource Manager 27-2

MTP Types in Cisco Unified CallManager Administration 27-3

Planning Your Software MTP Configuration 27-3

Software MTP Device Characteristics 27-4

Avoiding Call Failure/User Alert 27-4

MTP System Requirements and Limitations 27-5

MTP Failover and Fallback 27-5

Active Cisco Unified CallManager Becomes Inactive 27-5

Resetting Registered MTP Devices 27-6

Dependency Records 27-6

Software MTP Performance Monitoring and Troubleshooting 27-6

Software MTP Configuration Checklist 27-7

Where to Find More Information 27-7

CHAPTER 28 Cisco DSP Resources for Transcoding, Conferencing, and MTP 28-1

Understanding Cisco DSP Resources 28-1

Hardware-Based MTP/ Transcoding Services 28-2

IP-to-IP Packet Transcoding and Voice Compression 28-3

Voice Compression, IP-to-IP Packet Transcoding, and Conferencing 28-3

IP-to-IP Packet Transcoding Across Intercluster Trunks 28-4

Hardware-Based Conferencing Services 28-4

Supported Cisco Catalyst Gateways and Cisco Access Routers 28-5

Cisco Catalyst 4000 WS-X4604-GWY 28-5

Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1 28-6

Cisco 2600, Cisco 2600XM, Cisco 2800, Cisco 3600, Cisco 3700, Cisco 3800, and Cisco VG200 for NM-HDV 28-8

Cisco 2600XM, Cisco 2691, Cisco 2800, Cisco 3600, Cisco 3700, and Cisco 3800 for NM-HD and NM-HDV2 28-8

Where to Find More Information 28-10

PART 6 Voice Mail and Messaging Integration

CHAPTER 29 Voice Mail Connectivity to Cisco Unified CallManager 29-1

Voice-Mail Interfaces 29-1

Voice-Mail System Access 29-2

Voice-Mail Pilot Numbers 29-3

Voice-Mail Profiles 29-3

Message Waiting 29-4

Message Waiting Indication 29-4

Call Forwarding in a Multiple Voice-Mail System Environment 29-5

Call Transfer with Voice-Mail Systems 29-6

Where to Find More Information 29-7

CHAPTER 30 SMDI Voice Mail Integration 30-1

SMDI Voice Mail Integration Requirements 30-1

Port Configuration for SMDI 30-2

Cisco Messaging Interface Redundancy 30-2

SMDI Configuration Checklist 30-4

Where to Find More Information 30-5

CHAPTER 31 **Cisco Unity Messaging Integration** 31-1

System Requirements 31-1

Integration Description 31-2

Cisco Unified CallManager SIP Trunk Integration 31-3

Cisco Unity Cisco Unified CallManager Integrated Mailbox Configuration 31-4

Securing the Voice-Mail Port 31-4

Cisco Unity Configuration Checklist 31-5

Where to Find More Information 31-7

CHAPTER 32 **Cisco DPA Integration** 32-1

Understanding the DPA 7630/7610 32-1

How the DPA 7630/7610 Works 32-2

Why is the DPA 7630/7610 Needed? 32-2

Can I Just Use SMDI? 32-2

What If I Cannot Use SMDI? 32-3

Where to Find More Information 32-3

PART 7 **System Features**

CHAPTER 33 **Call Park** 33-1

CHAPTER 34 **Call Pickup Group** 34-1

CHAPTER 35 **Cisco Unified IP Phone Services** 35-1

Understanding Cisco Unified IP Phone Services 35-1

Guidelines and Tips 35-2

Dependency Records 35-3

Cisco Unified IP Phone Service Configuration Checklist 35-3

Where to Find More Information 35-4

CHAPTER 36 **Cisco Extension Mobility and Phone Login Features** 36-1

CHAPTER 37 **Cisco Unified CallManager Attendant Console** 37-1

CHAPTER 38 **Cisco Unified CallManager Assistant** 38-1

PART 8 **Devices and Protocols**

CHAPTER 39 **Understanding Cisco Unified CallManager Voice Gateways** 39-1

Cisco Voice Gateways 39-1

Standalone Voice Gateways 39-2

Cisco Voice Gateway 200 39-2

Cisco Access Digital Trunk Gateways DT-24+/DE-30+ 39-2

Cisco VG248 Analog Phone Gateway 39-2

Cisco VG224 Analog Phone Gateway 39-4

Cisco IAD2400 Series Integrated Access Device 39-4

MGCP BRI Call Connections 39-4

Cisco Catalyst 4000 and 6000 Voice Gateway Modules 39-5

Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module 39-6

Cisco Catalyst 6000 24 Port FXS Analog Interface Module 39-6

Cisco Communication Media Module 39-7

Cisco Catalyst 4000 Access Gateway Module 39-7

Cisco Catalyst 4224 Voice Gateway Switch 39-7

H.323 Gateways 39-7

Cisco IOS H.323 Gateways 39-7

T.38 Fax Relay 39-8

Outbound FastStart Call Connections 39-8

Voice Gateway Model Summary 39-9

Gateways, Dial Plans, and Route Groups 39-12

Dependency Records for Gateways and their Route Groups and Directory Numbers 39-13

Gateway Failover and Fallback 39-13

MGCP Gateways 39-13

IOS H.323 Gateways 39-14

Cisco VG248 Analog Phone Gateway 39-14

Transferring Calls Between Gateways 39-14

Configuring Transfer Capabilities Using Gateway Configuration 39-15

Configuring Transfer Capabilities by Using Call Classification Service Parameter 39-15

Blocking Transfer Capabilities by Using Service Parameters 39-16

Gateway Configuration Checklist 39-16

MGCP BRI Gateway Configuration Checklist 39-18

Where to Find More Information 39-18

CHAPTER 40 Understanding IP Telephony Protocols 40-1

IP Protocols 40-1

H.323 Protocol 40-1

Media Gateway Control Protocol (MGCP) 40-2

Skinny Client Control Protocol (SCCP) 40-2

Session Initiation Protocol (SIP) 40-3

Analog Telephony Protocols 40-3

Loop-Start Signaling 40-4

Ground-Start Signaling 40-4

E&M Signaling 40-4

Channel Associated Signaling (CAS) 40-5

T1 CAS 40-5

E1 CAS 40-5

Digital Telephony Protocols 40-5

Basic Rate Interface (BRI) 40-6

T1 Primary Rate Interface (T1 PRI) 40-6

E1 Primary Rate Interface (E1 PRI) 40-6

Q.Signaling (QSIG) 40-6

Annex M.1 (Message Tunneling for QSIG) 40-7

Basic Call for QSIG 40-8

Call Completion 40-8

Call Diversion 40-9

Call Transfer 40-10

Compatibility with Older Versions of QSIG Protocol (ECMA) 40-10

Facility Selection and Reservation 40-11

Identification Services 40-11

Message Waiting Indication (MWI) Service 40-13

Path Replacement 40-13

QSIG Interface to Cisco Unified CallManager 40-15

Where to Find More Information 40-15

CHAPTER 41 Understanding Session Initiation Protocol (SIP) 41-1

SIP Networks 41-1

SIP and Cisco Unified CallManager 41-2

Media Termination Point (MTP) Devices 41-3

SIP Service Parameters 41-3

SIP Timers and Counters 41-3

Supported Audio Media Types 41-4

Supported Video Media Types 41-4

Supported Application Media Type 41-5

Supported T38fax Payload Type 41-5

SIP Profiles for Trunks 41-5

SIP Functions That Are Supported in Cisco Unified CallManager 41-5

Basic Calls Between SIP Endpoints and Cisco Unified CallManager 41-6

Basic Outgoing Call 41-6

Basic Incoming Call 41-6

Use of Early Media 41-6

DTMF Relay Calls Between SIP Endpoints and Cisco Unified CallManager 41-6

Forwarding DTMF Digits from SIP Devices to Gateways or Interactive Voice Response (IVR) Systems for Dissimilar DTMF methods 41-7

Generating DTMF Digits for Dissimilar DTMF Methods 41-7

Supplementary Services That Are Initiated If an MTP Is Allocated 41-8

Ringback Tone During Blind Transfer 41-8

Supplementary Services That Are Initiated by SIP Endpoint 41-9

SIP–Initiated Call Transfer 41-9

Call Hold 41-9

Call Forward 41-9

Enhanced Call Identification Services 41-9

Calling Line and Name Identification Presentation 41-10

Calling Line and Name Identification Restriction 41-10

Connected Line and Name Identification Presentation 41-11

Connected Line and Name Identification Restriction 41-11

Redirecting Dial Number Identification Service (RDNIS) 41-12

Redirection 41-12

SIP Trunk Configuration Checklist 41-13

Cisco Unified CallManager SIP Endpoints Overview 41-13

SIP Line Side Overview 41-15

SIP Standards 41-15

RFC3261, RFC3262 (PRACK), RFC3264 (offer/answer), RFC3311 (UPDATE), 3PCC 41-15

RFC3515 (REFER) also Replaces and Referred-by Headers 41-16

Remote Party Id (RPID) Header 41-16

Diversion Header 41-16

Replaces Header 41-16

Join Header 41-16

RFC3265 + Dialog Package 41-17

RFC3265 + Presence Package 41-17

RFC3265 + KPML Package 41-17

RFC3265 + RFC3842 MWI Package (unsolicited notify) 41-17

Remotecc 41-17
RFC4028 Session Timers 41-17
Cisco Unified CallManager Functionality Supported by SIP Phones 41-18
Dial Plans 41-18
PLAR 41-18
Softkey Handling 41-18
DSCP Configuration 41-19
SIP Profiles for Endpoints 41-19
Network Time Protocol (NTP) 41-19
Where to Find More Information 41-20

CHAPTER 42 Understanding Cisco Unified CallManager Trunk Types 42-1
Cisco Unified CallManager Trunk Configuration 42-1
Trunks and Gatekeepers in Cisco Unified CallManager 42-2
Gatekeeper-Controlled Trunks 42-2
Non-Gatekeeper-Controlled Trunks 42-2
Trunk Types in Cisco Unified CallManager Administration 42-2
H.225 Trunk (Gatekeeper Controlled) 42-3
Intercluster Trunk (Gatekeeper Controlled) 42-3
Intercluster Trunk (Non-Gatekeeper Controlled) 42-3
SIP Trunk 42-3
Transferring Calls Between Trunks 42-4
Configuring Transfer Capabilities Using Trunk Configuration 42-4
Configuring Transfer Capabilities by Using Call Classification Service Parameter 42-5
Blocking Transfer Capabilities by Using Service Parameters 42-5
Dependency Records for Trunks and Associated Route Groups 42-6
Trunk Configuration Checklist 42-6
Where to Find More Information 42-7

CHAPTER 43 Cisco Unified IP Phones 43-1
Supported Cisco Unified IP Phones 43-2
Cisco SIP IP Phones 43-7
H.323 Clients and CTI Ports 43-8
Cisco IP Communicator 43-8
Cisco Unified Personal Communicator 43-8
Phone Button Templates 43-9
Default Phone Button Templates 43-10
Guidelines for Customizing Phone Button Templates 43-13

Softkey Templates 43-15

Add Application 43-16

Configure Softkey Layout 43-17

Softkey Template Operation 43-18

Common Phone Profiles 43-19

Methods for Adding Phones 43-19

Phone Features 43-20

Phone Association 43-25

Phone Administration Tips 43-25

Phone Search 43-26

Messages Button 43-27

Directories Button 43-28

Cisco Unified CallManager User Options 43-28

Maximum Phone Fallback Queue Depth Service Parameter 43-28

Dependency Records 43-29

Phone Failover and Fallback 43-29

Phone Configuration Checklist 43-29

Where to Find More Information 43-33

CHAPTER 44 Understanding Video Telephony 44-1

Introducing Video Telephony 44-1

Video Calls 44-2

Video Codecs 44-2

Video Network 44-3

Enabling an Audio-Only Device with Video 44-4

H.323 Video 44-4

Dynamic H.323 Addressing 44-5

Registering with the Gatekeeper 44-5

Call Processing 44-5

Configuration Notes 44-6

Skinny Client Control Protocol Video 44-6

Skinny Client Control Protocol Video Bridging 44-6

SIP Video 44-7

Configuring a SIP Trunk for Video Calls 44-7

Bandwidth Management 44-7

Regions 44-8

Locations 44-8

RSVP 44-8

Alternate Routing 44-8

DSCP Marking 44-8

Phone Configuration for Video Calls 44-9

Additional Configuration for Video Calls 44-9

Trunk Interaction with H.323 Client 44-9

Call Routing for Video Calls 44-9

Gateway Timer Parameter 44-9

Conference Control for Video Conferencing 44-9

Video Telephony and Cisco Serviceability 44-10

Performance Monitoring Counters 44-10

Video Bridge Counters 44-11

Call Detail Records 44-11

Video Telephony Configuration Checklist 44-12

Where to Find More Information 44-13

CHAPTER 45 **Computer Telephony Integration** 45-1

Computer Telephony Integration Applications 45-1

CTIManager 45-2

Media Termination Points 45-2

CTI-Controlled Devices 45-3

User Management and CTI Controlled Devices 45-5

Applications That Monitor and Control All CTI-Controllable Devices 45-5

Dependency Records 45-6

CTI Redundancy 45-6

Cisco Unified CallManager 45-6

CTIManager 45-7

Application Failure 45-7

CTI Configuration Checklist 45-8

Where to Find More Information 45-9

CHAPTER 46 **Cisco ATA 186** 46-1

Cisco ATA 186 Features 46-1

Connecting with Cisco Unified CallManager 46-1

Configuration Checklist 46-2

Where to Find More Information 46-2

PART 9

System Maintenance

CHAPTER 47 Administrative Tools Overview 47-1

Bulk Administration Tool (BAT) 47-1

Cisco Unified CallManager Serviceability 47-1

CDR Analysis and Reporting (CAR) 47-2

Call Detail Records 47-2

Where to Find More Information 47-3

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

Purpose

The *Cisco Unified CallManager System Guide* provides conceptual information about Cisco Unified CallManager and its components as well as tips for setting up features by using Cisco Unified CallManager Administration. This book acts as a companion to the *Cisco Unified CallManager Administration Guide*, which provides instructions for administering the Cisco Unified CallManager system, including descriptions of procedural tasks that you complete by using Cisco Unified CallManager Administration.

Audience

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

Organization

The following table shows the organization of this guide:

Part	Description
Part 1	"Understanding Cisco Unified CallManager" Provides an overview of Cisco Unified CallManager and Cisco Unified Communications network components.
Part 2	"Understanding Cisco Unified CallManager System Configuration" Details the basic configuration flow for a Cisco Unified CallManager system and explains system-level configuration concepts and settings.
Part 3	"Dial Plan Architecture" Describes route plans, partitions, calling search spaces, time-of-day routing, directory numbers, and dial rules.
Part 4	"LDAP Directory and User Configuration" Provides information about the LDAP directory and configuration of application users and end users.
Part 5	"Media Resources" Explains how to manage and configure media resources such as transcoders, annunciators, conference bridges, media termination points, music on hold audio sources, and music on hold servers.
Part 6	"Voice Mail and Messaging Integration" Discusses how to integrate voice mail and messaging applications with Cisco Unified CallManager.
Part 7	"System Features" Describes additional system-wide features such as call park, call pickup, and Cisco Unified IP Phone services.
Part 8	"Devices and Protocols" Explains how to configure supported voice gateways, protocols, Cisco Unified IP Phones, video telephony, and software applications for Cisco Unified CallManager.
Part 9	"System Maintenance" Describes administrative tools and system maintenance for your Cisco Unified CallManager system.

Related Documentation

Refer to the following documents for further information about related Cisco Unified Communications applications and products:

- *Installing Cisco Unified CallManager Release 5.0(4)*
- *Upgrading Cisco Unified CallManager Release 5.0(4)*
- *Release Notes for Cisco Unified CallManager Release 5.0(4)*
- *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Features and Services Guide*
- *Troubleshooting Guide for Cisco Unified CallManager*
- *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*
- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified 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.
→	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.

Notes use the following conventions:

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 conventions:

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

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

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 submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—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.

- For 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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*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.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- 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:

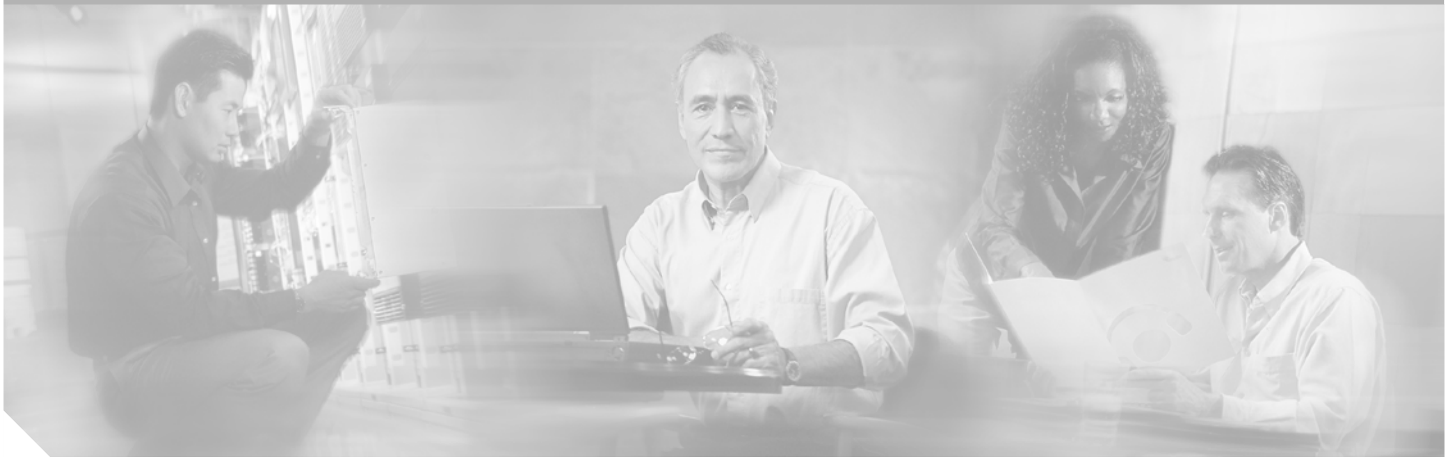
  http://www.cisco.com/en/US/products/index.html

- 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



Part 1

Understanding Cisco Unified CallManager

CHAPTER 1

Introduction

Cisco Unified CallManager serves as the software-based, call-processing component of Cisco Unified Communications. The Cisco Unified Communications Applications Server provides a high-availability server platform for Cisco Unified CallManager call processing, services, and applications.

The Cisco Unified CallManager system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco Unified CallManager open telephony application program interface (API).

Cisco Unified CallManager provides signaling and call control services to Cisco integrated telephony applications as well as to third-party applications. It performs the following primary functions:

- Call processing
- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services
- Operations, administration, management, and provisioning (OAM&P)
- Programming interface to external voice-processing applications such as Cisco IP Communicator, Cisco Unified IP Interactive Voice Response (IP IVR), and Cisco Unified CallManager Attendant Console

Cisco Unified CallManager as an Appliance

Cisco Unified CallManager release 5.0 works as an Appliance on a non-Windows-based Operating System. The Cisco Unified CallManager appliance refers to the following functions:

- Works on a specific hardware platform(s) that Cisco specifies and supplies and, in some cases, the customer supplies
- Works in a carefully controlled software environment that Cisco specifies and installs
- Includes all software that is required to operate, maintain, secure, and manage a server or cluster of servers (including Cisco Security Agent)

- Outputs a variety of management parameters via a published interface to provide information to approved management applications such as, but not limited to, NetIQ Vivinet Manager, HP Openview, and Integrated Research Prognosis
- Operates in a headless manner (without keyboard, mouse, or VGA monitor support) or (in the case of some of the hardware platforms) in a headed manner (with keyboard, mouse, and monitor)
- Exposed interfaces:
  - Ethernet to the network
  - Web interface for Platform and Cisco Unified CallManager Administration
  - Command Line Interface (CLI) based platform shell for administrator use
  - APIs such as JTAPI, AXL/SOAP, and SNMP for third-party application and management support
- Cisco Unified CallManager servers get preinstalled with software to ease customer and partner deployment and automatically search for updates and notify administrators when key security fixes and software upgrades are available for their system. This process comprises Electronic Software Delivery.
- You can upgrade Cisco Unified CallManager servers while they continue to process calls, so upgrades takes place with minimal downtime.
- Cisco Unified CallManager supports the Asian and Middle Eastern markets by providing support for Unicode on higher resolution phone displays.
- Cisco Unified CallManager provides Fault, Configuration, Accounting, Performance, and Security (FCAPS).

Key Features and Benefits

The Cisco Unified CallManager system includes a suite of integrated voice applications that perform voice conferencing and manual attendant console functions. Supplementary and enhanced services such as hold, transfer, forward, conference, multiple-line appearances, automatic route selection, speed dial, last-number redial, and other features extend to IP phones and gateways. Because Cisco Unified CallManager is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform, thereby avoiding expensive hardware upgrade costs.

Distribution of Cisco Unified CallManager and all Cisco Unified IP Phones, gateways, and applications across an IP network provides a distributed, virtual telephony network. This architecture improves system availability and scalability. Call admission control ensures that voice quality of service (QoS) is maintained across constricted WAN links and automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available.

A web-browsable interface to the configuration database provides the capability for remote device and system configuration. This interface also provides access to HTML-based online help for users and administrators.

Where to Find More Information

Additional Cisco Documentation

- *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Features and Services Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified Communications Solution Reference Network Design*
- *Cisco Unified Communications Operating System Administration Guide*
- *Disaster Recovery System Administration Guide*

Cisco Unified Communications Overview

Multiple communication networks exist as entirely separate entities, each serving a specific application. The traditional public switched telephone network (PSTN) time-division multiplexing (TDM) network serves the voice application; the Internet and intranets serve data communications.

Business requirements often force these networks to interoperate. As a result, deploying multiservice (data, voice, and video) applications such as unified messaging or web-based customer contact centers requires expensive and complex links between proprietary systems, such as private branch exchanges (PBXs) and standards-based data networks.

The traditional enterprise communication takes place on two separate networks:

- Voice
- Data

Internet Ecosystem

Over time, the Internet (and data networking technology in general) encompassed the traditional traffic types. This convergence recently started to absorb voice and video as applications into the data network. Several large Post, Telephone, and Telegraph (PTT) carriers use packet switching or voice over ATM as their backbone technology, and enterprise customers accept virtual trunking, or connect their disparate PBXs via their wide-area data network, to avoid long-distance charges.

Converging these previously disparate networks into a single, unified network realizes savings in multiple areas, including lower total cost of ownership, toll savings, and increased productivity.

Cisco Unified CallManager and Cisco Unified IP Phones provide an IP telephony solution that operates on an IP infrastructure. The clustering architecture of Cisco Unified CallManagers allows you to scale to a highly available voice-over-IP (VoIP) network.

Cisco Unified Communications Support

Cisco Unified Communications support encompasses the following components:

- Converged client devices
- Hardware/software
- Directory services
- Call processing

- Telephony/data applications
- Network management
- Service and support

Cisco Unified Communications solutions enable you to

- Deploy IP-enabled business applications
- Implement a standards-based open architecture
- Migrate to a converged network in your own time frame

Cisco Unified Communications support enables you to move from maintaining a separate data network and a closed, proprietary voice PBX system to maintaining one open and standards-based, converged network for all your data, voice, and video needs.

Applications

The following list includes the major Cisco Unified Communications voice and video applications:

- Cisco Unified CallManager—This software-only call-processing application distributes calls, features, phones, regions, and groups over an IP network.
- Cisco Unity—The Cisco Unity messaging application provides voice messaging to enterprise communications.
- Cisco Unity Connection. For more information about Cisco Unity Connection, refer to the *Cisco Unified CallManager 5.0 SCCP Integration Guide for Cisco Unity Connection 1.1* or the *Cisco Unified CallManager 5.0 SIP Trunk Integration Guide for Cisco Unity Connection 1.1*.
- Video—IP-TV and IP-video conferencing products enable distance learning and workgroup collaboration.
- Cisco Unified IP-IVR—As an IP-powered interactive voice response (IVR) solution, Cisco Unified IP-IVR, combined with Cisco IP AutoAttendant, provides an open and feature-rich foundation for delivering IVR solutions over an IP network.
- Cisco Unified CallManager Attendant Console—This flexible and scalable application replaces the traditional PBX manual attendant console.
- Cisco IP Communicator—The Cisco IP Communicator, a software, computer-based phone, provides communication capabilities that increase efficiency and promote collaboration.

Call Processing

Cisco Unified CallManager, a software-only call-processing application, distributes calls and features and clusters phones, regions, and groups over an IP network, which allows scalability to 30,000 users and triple call-processing redundancy.

Cisco Unified CallManager provides signaling and call-control services to Cisco-integrated applications, as well as to third-party applications.

Infrastructure

The following list shows the components of the infrastructure layer of Cisco Unified Communications:

- Media convergence servers
- General voice products for Cisco Unified Communications Solutions
- Switches
- Integrated IP telephony solution
- Voice trunks
- Voice gateways
- Toll bypass products
- IP protocols such as MGCP, H.323, and SIP

Clients

Cisco delivers the following IP-enabled communication devices:

- Cisco Unified IP Video Phone 7985—supports SCCP
- Cisco Unified IP Phone 7970/7971—supports SCCP and SIP protocols
- Cisco Unified IP Phone 7960/7961—supports SCCP and SIP protocols
- Cisco Unified IP Phone 7940/7941—supports SCCP and SIP protocols
- Cisco Unified Wireless IP Phone 7920—supports SCCP
- Cisco Unified IP Phone 7912—supports SCCP and SIP protocols
- Cisco Unified IP Phone 7911—supports SCCP and SIP protocols
- Cisco Unified IP Phone 7910—supports SCCP
- Cisco Unified IP Phone 7905—supports SCCP and SIP protocol
- Cisco Unified IP Phone 7902—supports SCCP
- Cisco Unified IP Conference Station 7936
- Cisco Unified IP Conference Station 7935
- Cisco IP Communicator
- Cisco Unified IP Phone Expansion Module 7914

Cisco also supports various third-party SIP phones. Contact your Cisco representative for more information.

Cisco Unified Communications Network

The Cisco Unified Communications network includes the following components:

- Cisco Unified CallManager
- Cisco Unified IP Phones
- IOS platforms

- Power Over Ethernet (POE) switches
- Digital gateways and trunks
- Analog gateways
- Transcoders
- Conferencing (hardware/software)
- Media Termination Point (MTP)
- Music On Hold (MOH)
- Annunciator
- Inline power modules (10/100 Ethernet switching modules)
- Cisco IP Communicator

Control from the Cisco Unified IP Phone to Cisco Unified CallManager uses skinny client control protocol and, independently, desktop computer to Cisco Unified CallManager, as an H.323 gatekeeper that is using H.225/H.245 over transmission control protocol (TCP).

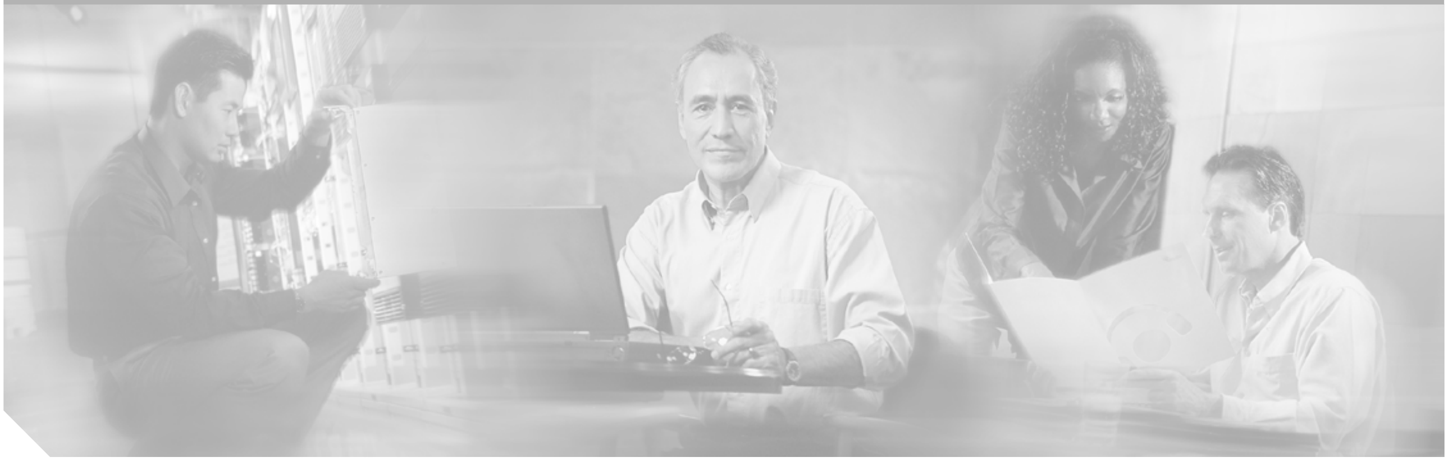
Where to Find More Information

Related Topics

- Introduction, page 1-1
- System Configuration Overview, page 3-1
- Device Support, page 11-1
- Understanding Cisco Unified CallManager Voice Gateways, page 39-1
- Transcoders, page 25-1
- Conference Bridges, page 24-1

Additional Cisco Documentation

- Cisco Unified CallManager Configuration, *Cisco Unified CallManager Administration Guide*
- Device Defaults Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide*
- Transcoder Configuration, *Cisco Unified CallManager Administration Guide*
- Conference Bridge Configuration, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Features and Services Guide*
- *Cisco Unified Communications Solution Reference Network Design Guide*
- Cisco Unified IP Phone user and administration documentation
- Gateway documentation



Part 2

Understanding Cisco Unified CallManager System Configuration

CHAPTER 3

System Configuration Overview

For best results when configuring a complete Cisco Unified Communications system, start with the system-level components and work toward the individual devices. For example, you have to configure the appropriate device pools, route lists, locations, and calling search spaces before you can use those components to configure phones and lines.

This chapter presents an overall flow, or order, for configuring the components of your Cisco Unified Communications network. It covers the following topics:

- Basic Configuration Flow, page 3-1
- Where to Find More Information, page 3-4

Basic Configuration Flow

Table 3-1 lists the general steps that are involved in configuring a complete IP telephony system. If you are not using a particular feature or component, you can skip that step. You have some flexibility in the order for performing these configuration steps, and in some cases, you might have to alternate between steps or return to a given step several times to complete your configuration.

Table 3-1 Configuration Overview Checklist

Configuration Steps		Procedures and related topics
Step 1	Install the Cisco Unified CallManager software on one server. This server acts as the database server and is referred to as the first server. Before installing any subsequent servers, always define the node in Server Configuration of Cisco Unified CallManager Administration. Security purposes requires this action.	*Installing Cisco Unified CallManager Release 5.0(4)* Server Configuration, *Cisco Unified CallManager Administration Guide*
Step 2	Install the Cisco Unified CallManager software on each subsequent server.	
Step 3	Add services, as required, to the first database server.	*Cisco Unified CallManager Serviceability Administration Guide* *Cisco Unified CallManager Serviceability System Guide*

Table 3-1 Configuration Overview Checklist (continued)

Configuration Steps		Procedures and related topics
Step 4	Configure system-level settings: • Cisco Unified CallManagers (Be aware that some Cisco Unified CallManager-specific elements are required, such as enabling of auto-registration and establishing a starting directory number [DN].) • Cisco Unified CallManager groups • Date/time groups • Regions • Softkey templates (Softkey templates represent a required field in device pool configuration, but they offer standard template options as well.) • Device defaults • Enterprise parameters • Locations	System-Level Configuration Settings, page 5-1
Step 5	Design and configure your dialing plan: • AAR Group • Application Dial Rules (optional, used by Cisco Unified CM Assistant and Cisco WebDialer) • Partitions • Calling search spaces • Route filters • Route groups and line groups • Route and hunt lists • Route patterns (If you want to assign route patterns to gateways, you need to create gateways prior to configuring the route pattern for those gateways.) • Translation patterns	Partitions and Calling Search Spaces, page 15-1 Understanding Route Plans, page 17-1
Step 6	Configure media resources: • Conference bridges • Transcoders • Annunciator • Media termination points • Music on hold audio sources • Music on hold servers • Media resource groups • Media resource group lists	Media Resource Management, page 22-1 Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide*

Table 3-1 Configuration Overview Checklist (continued)

Configuration Steps		Procedures and related topics
Step 7	Configure device pool settings: • Cisco Unified CallManager group • Date/Time group • Regions • Softkey template • SRST reference • Calling Search Space for Auto-registration • Media Resource Group List • Network Hold MOH Audio Source • User Hold MOH Audio Source • Network Locale • User Locale	Device Pool Configuration, *Cisco Unified CallManager Administration Guide*
Step 8	Install and configure one of the following voice-messaging systems: • External (non-Cisco) voice-messaging system • Cisco Unity voice-messaging system	SMDI Voice Mail Integration, page 30-1 Administration documentation for Cisco Unity
Step 9	Configure meet-me numbers/patterns.	Meet-Me Number/Pattern Configuration, *Cisco Unified CallManager Administration Guide*
Step 10	Configure message-waiting numbers.	Message Waiting Configuration, *Cisco Unified CallManager Administration Guide*
Step 11	Configure features: • Call park • Call pickup and group call pickup • Barge • Immediate Divert • Cisco IP phone services • Cisco Extension Mobility • Cisco Unified CallManager Attendant Console	Configuring Call Park, *Cisco Unified CallManager Features & Services Guide* Call Pickup Group, page 34-1 Configuring Barge and Privacy, *Cisco Unified CallManager Features and Services Guide* Configuring Immediate Divert, *Cisco Unified CallManager Features and Services Guide* Cisco Unified IP Phone Services, page 35-1 Cisco Extension Mobility, *Cisco Unified CallManager Features and Services Guide* Cisco Unified CallManager Attendant Console, page 37-1
Step 12	Install and configure the gateways.	Understanding Cisco Unified CallManager Voice Gateways, page 39-1

Table 3-1 Configuration Overview Checklist (continued)

Configuration Steps		Procedures and related topics
Step 13	Configure and install the phones; then, associate users with the phones. Also, configure phone button templates and softkey templates.	Cisco Unified IP Phones, page 43-1 Understanding the Directory, page 20-1 Phone Button Template Configuration, *Cisco Unified CallManager Administration Guide* Softkey Template Configuration, *Cisco Unified CallManager Administration Guide* Administration documentation for Cisco Unified IP Phones
Step 14	Enable computer telephony integration (CTI) application support; then, install and configure the desired CTI applications.	Computer Telephony Integration, page 45-1 Documentation provided with your application

Where to Find More Information

Related Topic

- See Table 3-1.

Additional Cisco Documentation

- *Installing Cisco Unified CallManager Release 5.0(4)*
- *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Features and Services Guide*
- Administration documentation for Cisco Unified IP Phones

Roles and User Groups

Cisco Unified CallManager Administration uses roles and user groups to provide varying levels of privilege (access). This technique permits granting only the required privileges for a selected group of users and limits the configuration functions that users in a particular user group can perform.

Use the following topics to understand roles and user groups:

- Overview, page 4-1
- Roles, page 4-2
- Role Access Privileges, page 4-2
- User Groups, page 4-3
- Access Log, page 4-3
- Enterprise Parameters, page 4-3
- Standard Roles and User Groups, page 4-4
- Where to Find More Information, page 4-4

Related Topics

- Role Configuration, *Cisco Unified CallManager Administration Guide*
- User Group Configuration, *Cisco Unified CallManager Administration Guide*

Overview

Roles and user groups provide multiple levels of security to Cisco Unified CallManager Administration and to other applications. The system groups the resources that are available to Cisco Unified CallManager Administration and to other applications into roles. Each application comes with standard, predefined roles. Each application defines its own access privilege for Cisco Unified CallManager Administration.

Administrators can configure additional roles for an application. A role contains, for a particular application, the list of resources that an application comprises. For each resource that a role comprises, the administrator defines the access privilege. For the Cisco Unified CallManager Administration application, the access privileges include *read* and *update*. Other applications specify their own access privileges.

After configuration of roles for an application, administrators can configure user groups. User groups define groups of users that share a common list of assigned roles. User groups comprise both application users and end users.

Roles

A role includes a collection of resources for an application, such as the Cisco Unified CallManager Administration application. Two types of roles exist: standard roles, which are the default roles, and custom, administrator-defined roles. Standard roles for an application get created upon installation of the application. Administrators may define custom roles.

Note All standard roles get created at installation. You cannot modify or delete standard roles, but you can copy them to create new custom roles based on standard roles.

Role Access Privileges

For the Cisco Unified CallManager Administration application, one of the following access privileges applies to the resources that a particular role comprises:

- Read
- Update

Note Other applications specify their own access privileges.

For each role that is associated with the Cisco Unified CallManager Administration application, one of these privilege levels applies for access to each of the resources. The access privileges specify the following privileges:

- Access privilege *Read* specifies that users in a user group that have this privilege defined for a particular resource can view only the windows that the resource comprises but cannot modify the windows. Access privilege *Read* limits access to windows to read operations. Buttons such as **Insert**, **Delete**, **Update**, and **Reset** do not display.
- Access privilege *Update* specifies that users in a user group that this privilege defined for a particular resource can view and change the windows that the resource comprises. Users with update privilege can perform operations such as Insert, Delete, Update, and Reset, as well as executive functions that can start or stop a process or service from the Cisco Unified CallManager Administration and Serviceability windows.

For each application, install assigns default access privileges to the roles that get created at install time.

Note The Standard CCM Admin Users role gives the user access to the Cisco Unified CallManager Administration user interface. This role, the base role for all administration tasks, serves as the authentication role. Cisco Unified CallManager Administration defines this role as the role that is necessary to log in to Cisco Unified CallManager Administration.

The Standard CCM Admin Users role includes no permissions beyond logging into Cisco Unified CallManager Administration. The administrator must add another authorization role to define the parts of the Cisco Unified CallManager Administration that the user can administer. The Standard CCMADMIN Administration role allows a user to access and make changes in all of Cisco Unified CallManager Administration.

Note A user with only the Standard CCM Admin Users role can access Cisco Unified CallManager Administration but cannot make any changes. A user with only the Standard CCMADMIN Administration role can make changes, but cannot authenticate entry to Cisco Unified CallManager Administration.

A user, therefore, must have the Standard CCM Admin User role to access Cisco Unified CallManager Administration and must have at least one other role to administer the system.

User Groups

A user group comprises a collection of Cisco Unified CallManager application users and end users that are grouped together for the purpose of assigning a common list of roles to the members in the user group.

Various named user groups that are predefined have no members that are assigned to them at install time. The Cisco Unified CallManager super user or a user with access to user group configuration should add users to these groups. The super user or a user with access to user group configuration can configure additional named user groups as needed.

Note The standard CCM Super Users user group represents a named user group that always has full access permission to all named roles. You cannot delete this user group. You can only make additions and deletions of users to this group.

Note CCMAdministrator always represents a super user.

For the complete listing of user groups, see the "Standard Roles and User Groups" section on page 4-4.

Access Log

The log contains a file report of access/change attempts. That is, Cisco Unified CallManager Administration generates a record of attempts to access or modify any directory or database component through Cisco Unified CallManager Administration. The change record includes the user name, date, time, window from which the change was made, and the success or failure status of the update.

Enterprise Parameters

Roles and user groups use the Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter.

Effective Access Privileges for Overlapping User Groups and Roles

The Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter determines the level of user access for users that belong to multiple user groups and have conflicting privileges.

You can set this enterprise parameter to the following values:

- Maximum—The effective privilege represents the maximum of the privileges of all the overlapping user groups.
- Minimum—The effective privilege represents the minimum of the privileges of all the overlapping user groups.

The Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter specifies the Maximum default value.

Note This enterprise parameter does not affect the privileges for the members of the standard CCM Super Users user group.

Standard Roles and User Groups

When you install Cisco Unified CallManager Administration, standard roles and standard user groups get created. Be aware that the list of standard roles and standard user groups is dynamic.

Standard user groups in Cisco Unified CallManager Administration provide a predefined set of roles and permissions for various functions. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. Administrators can disable functions that they do not use or modify standard functions to increase security.

Because Cisco Unified CallManager allows administrators to manage user groups, roles, and resources, no guarantee exists that a particular user group or role goes unchanged or that administrators will use the predefined user groups or roles.

Certain user groups and roles exhibit limitations that administrators need to recognize, particularly user groups and roles that concern applications. For example, you can modify the Standard EM Authentication Proxy Rights user group by adding both application users and end users. Because authentication by proxy is intended for use by applications, end users that get added to this user group cannot authenticate by proxy.

You cannot delete standard roles and standard user groups, but the CCMAdministrator can modify a standard role or a standard user group.

Where to Find More Information

Related Topics

- Role Configuration, *Cisco Unified CallManager Administration Guide*
- User Group Configuration, *Cisco Unified CallManager Administration Guide*
- Application Users and End Users, page 21-1
- Application User Configuration, *Cisco Unified CallManager Administration Guide*
- End User Configuration, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- *Installing Cisco Unified CallManager*
- *Cisco Unified CallManager Administration Guide*

- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*

CHAPTER 5

System-Level Configuration Settings

Configure system-level settings before you add devices and configure other Cisco Unified CallManager features. This section covers the following topics:

- Server Configuration, page 5-1
- Cisco Unified CallManager Configuration, page 5-2
- Cisco Unified CallManager Groups, page 5-3
- Phone NTP Reference Configuration for SIP Phones, page 5-4
- Date/Time Groups, page 5-4
- Regions, page 5-5
- Device Pools, page 5-10
- LDAP, page 5-12
- Call Admission Control, page 5-13
- Survivable Remote Site Telephony References, page 5-13
- MLPP Domain, page 5-15
- Enterprise Parameters, page 5-15
- Service Parameters, page 5-16
- System Configuration Checklist, page 5-17
- Dependency Records, page 5-16
- Where to Find More Information, page 5-18

Server Configuration

Use the server configuration to specify the address of the server where Cisco Unified CallManager is installed. If your network uses Domain Name System (DNS) services, you can specify the host name of the server. If your network does not use DNS services, you must specify the Internet Protocol (IP) address of the server.

Note You must update the DNS server with the appropriate Cisco Unified CallManager name and address information before using that information to configure the Cisco Unified CallManager server.

Adding a Server

The following guidelines apply to adding a server:

- When you perform a fresh installation of Cisco Unified CallManager, you must define any subsequent servers (nodes) in the Cisco Unified CallManager Administration Server Configuration window before you can install the Cisco Unified CallManager software on each subsequent server. To define a subsequent node, click **Add New** and then configure the server. After you add the subsequent server, you can then install the Cisco Unified CallManager software on that server.
- Add each server only once on the Server Configuration window. If you add a server by using the host name and add the same server by using the IP address, Cisco Unified CallManager cannot accurately determine component versions for the server after a Cisco Unified CallManager upgrade. If you have two entries in Cisco Unified CallManager Administration for the same server, delete one of the entries before you upgrade the system.
- Any changes that you make to the server configuration do not take effect until you restart Cisco Unified CallManager.

Deleting a Server

Note You cannot delete a server that has a specific Cisco Unified CallManager that is running on it.

To find out which Cisco Unified CallManagers are using the server, choose **Dependency Records** from the Related Links drop-down list box on the Server Configuration window and click **Go**.

Before deleting a server that is currently in use, you must perform the following tasks:

- Update the Cisco Unified CallManager in question and assign it to a different server or delete the Cisco Unified CallManager that is assigned to that server.
- Delete the conference bridges, MTPs, and MOH servers that use the server that you want to delete.

  Note The system may automatically delete some devices, such as MOH servers, when you delete a server.

- Deactivate the services that are running on that server.

For more information, refer to the *Cisco Unified CallManager Administration Guide*, the *Cisco Unified CallManager Serviceability Administration Guide*, and the *Cisco Unified CallManager Features and Services Guide*.

Cisco Unified CallManager Configuration

The Cisco Unified CallManager servers get added to Cisco Unified CallManager at installation time. Use Cisco Unified CallManager configuration to update fields such as the ports and other properties for each Cisco Unified CallManager that is installed in the same cluster. A cluster comprises a set of Cisco Unified CallManagers that enables redundancy.

Any changes that you make to the settings for auto-registration partition, external phone number mask, and voice message box mask do not take effect until you restart Cisco Unified CallManager.

Note When you perform a fresh installation of Cisco Unified CallManager, you must activate the Cisco Unified CallManager service. For information about activating the Cisco Unified CallManager service, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Cisco Unified CallManager Groups

A Cisco Unified CallManager group comprises a prioritized list of up to three Cisco Unified CallManagers. The first Cisco Unified CallManager in the list serves as the primary Cisco Unified CallManager for that group, and the other members of the group serve as secondary (backup) Cisco Unified CallManagers.

Cisco Unified CallManager groups associate with devices through device pools. Each device belongs to a device pool, and each device pool specifies the Cisco Unified CallManager group for all of its devices.

Note Some Media Gateway Control Protocol (MGCP) devices, such as gateways and route/hunt lists, can associate directly with Cisco Unified CallManager groups.

Cisco Unified CallManager groups provide two important features for your system:

- Prioritized failover list for backup call processing—When a device registers, it attempts to connect to the primary (first) Cisco Unified CallManager in the group that is assigned to its device pool. If the primary Cisco Unified CallManager is not available, the device tries to connect to the next Cisco Unified CallManager that is listed in the group, and so on. Each device pool has one Cisco Unified CallManager group that is assigned to it.
- Call processing load balancing—You can configure device pools and Cisco Unified CallManager groups to distribute the control of devices across multiple Cisco Unified CallManagers. See the "Balanced Call Processing" section on page 6-3 for more information.

For most systems, you will assign a single Cisco Unified CallManager to multiple groups to achieve better load distribution and redundancy.

Adding a Cisco Unified CallManager Group

- Cisco Unified CallManagers are automatically installed and configured.
- Each Cisco Unified CallManager cluster can have only one default auto-registration group. If you choose a different Cisco Unified CallManager group as the default auto-registration group, the previously chosen auto-registration group no longer serves as the default for the cluster.
- You must reset the devices that use the updated Cisco Unified CallManager group to apply any changes that you make.

Deleting a Cisco Unified CallManager Group

Note You cannot delete a Cisco Unified CallManager group if it is assigned to any device pools or MGCP gateways or if it is the current Auto-registration Cisco Unified CallManager Group for the cluster.

To find out which devices are using the Cisco Unified CallManager group, choose **Dependency Records** from the Related Links drop-down list box on the Cisco Unified CallManager Group Configuration window and click **Go**.

Before deleting a Cisco Unified CallManager group that is currently in use, you must perform some or all of the following tasks:

- Assign a different Cisco Unified CallManager group to the device pools or MGCP gateways that currently use this Cisco Unified CallManager group.
- Create or choose a different Cisco Unified CallManager group to be the Auto-registration Cisco Unified CallManager Group.

For more information, refer to the *Cisco Unified CallManager Administration Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Phone NTP Reference Configuration for SIP Phones

You can configure phone Network Time Protocol (NTP) references in Cisco Unified CallManager Administration to ensure that a Cisco SIP IP Phone gets its date and time from an NTP server. If a SIP phone cannot get its date/time from the provisioned “Phone NTP Reference,” the phone will receive this information when it registers with Cisco Unified CallManager.

Adding a Phone NTP Reference

After you add the phone NTP reference to Cisco Unified CallManager Administration, you must add it to a date/time group. In the date/time group, you prioritize the phone NTP references, starting with the first server that you want the phone to contact.

The date/time group configuration gets specified in the device pool, and the device pool gets specified on the phone window.

Deleting a Phone NTP Reference

Before you can delete a phone NTP reference from Cisco Unified CallManager Administration, you must delete the server from the date/time group. To find which date/time groups use the phone NTP reference, choose **Dependency Records** from the Related Links drop-down list box in the Phone NTP Reference Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature. For more information about dependency records, refer to the “Dependency Records” section in the *Cisco Unified CallManager Administration Guide*.

Date/Time Groups

Use Date/Time Groups to define time zones for the various devices that are connected to Cisco Unified CallManager.

Cisco Unified CallManager provides a default Date/Time Group that is called CMLocal that configures automatically when you install Cisco Unified CallManager; however, Cisco recommends that you configure a group for each local time zone. CMLocal synchronizes to the active date and time of the operating system on the Cisco Unified CallManager server. After installing Cisco Unified CallManager, you can change the settings for CMLocal as desired. Normally, you adjust the server date/time to the local time zone date and time.

Note CMLocal resets to the operating system date and time whenever you restart Cisco Unified CallManager or upgrade the Cisco Unified CallManager software to a new release. Do not change the name of CMLocal.

Tip For a worldwide distribution of Cisco Unified IP Phones, create a Date/Time Group for each of the 24 time zones.

Adding a Date/Time Group

After adding a new date/time group to the database, you can assign it to a device pool to configure the date and time information for that device pool.

You must reset devices to apply any changes that you make.

Deleting a Date/Time Group

Note You cannot delete a date/time group that any device pool uses.

To find out which device pools use the Date/Time Group, choose **Dependency Records** from the Related Links drop-down list box on the Date/Time Group Configuration window and click **Go**.

Before deleting a Date/Time Group that is currently in use, you must perform either or both of the following tasks:

- Assign a different Date/Time Group to device pools that use the Date/Time Group that you want to delete.
- Delete the device pools that use the Date/Time Group that you want to delete.

For more information, refer to the *Cisco Unified CallManager Administration Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Regions

Use regions to specify the bandwidth that is used for audio and video calls within a region and between existing regions.

- The audio codec determines the type of compression and the maximum amount of bandwidth that is used per audio call.
- The video call bandwidth comprises the sum of the audio bandwidth and video bandwidth but does not include overhead.

When you create a region, you specify the codec that can be used for calls between devices within that region, and between that region and other regions. The system uses regions also for applications that only support a specific codec; for example, an application that only uses G.711.

The audio codec type specifies the technology that is used to compress and decompress voice signals. The choice of audio codec determines the compression type and amount of bandwidth that is used per call. See Table 5-1 for specific information about bandwidth usage for available audio codecs.

Note The default audio codec for all calls through Cisco Unified CallManager specifies G.711. If you do not plan to use any other audio codec, you do not need to use regions.

Cisco Unified CallManager supports video stream encryption and various audio/video codecs, such as G.722.

Regions provide capacity controls for Cisco Unified CallManager multisite deployments where you may need to limit the bandwidth for individual calls that are sent across a WAN link, but where you want to use a higher bandwidth for internal calls.

Adding a Region

To specify audio codec usage for devices that are using regions, you must perform the following tasks:

- Configure the default values for audio codec and video call bandwidth in the Cisco Unified CallManager Administration Service Parameters Configuration window.
- Create regions and specify the audio codecs to use for calls within those regions and between other regions.
- Create or modify device pools to use the regions that you created.
- Assign devices to device pools that specify the appropriate region.

Note Cisco Unified CallManager allows addition of a maximum of 500 regions.

Configuring Default Values

Region entries contain two values—audio codec and video call bandwidth.

- Audio Codec—You define audio codec values to be used within the same region, and you also define audio codec values to be used between regions.
- Video Call Bandwidth—You define video call bandwidth values to be used within the same region, and you also define video call bandwidth values to be used between regions.

Tip If you set both the audio codec values and the video call bandwidth values to use the default, the system uses less resources.

You configure the default values for regions in the Cisco Unified CallManager Administration Service Parameters window (**System > Service Parameters**).

- Regions have default values for use within a region—The recommended default value specifies G.711.
- Regions have default values for use between regions—The recommended default value specifies G.729.

Note For enhanced scalability, Cisco recommends that you properly set the default values in the Cisco Unified CallManager Administration Service Parameters Configuration window for both the audio codec and the video call bandwidth values, and then choose the Default settings in the Cisco Unified CallManager Administration Region Configuration window.

For more information about configuring regions, refer to Region Configuration in the *Cisco Unified CallManager Administration Guide.*

See the "Device Pools" section on page 5-10 for more information about device pool settings. For information about codes and video calls, see Understanding Video Telephony.

After adding a new region to the database, you can use it to configure device pools. Devices acquire a region setting from the device pool to which they are assigned.

Note To apply any changes that you make to all devices that use the updated region, you must restart the devices.

Supported Audio Codecs and Bandwidth Usage

Cisco Unified CallManager supports the following audio codecs for use with the regions feature:

- **G.711**—Default codec for all calls through Cisco Unified CallManager.
- **G.722**—Audio codec often used in video conferences.
- **G.723**—Low-bit-rate codec with 6-kbps compression for Cisco IP Phone model 12 SP+ and Cisco IP Phone model 30 VIP devices.
- **G.728**—Low-bit-rate codec that video endpoints support.
- **G.729**—Low-bit-rate codec with 8-kbps compression supported by Cisco Unified IP Phone 7900 models. Typically, you would use low-bit-rate codecs for calls across a WAN link because they use less bandwidth. For example, a multisite WAN with centralized call processing can set up a G.711 and a G.729 region per site to permit placing intrasite calls as G.711 and placing intersite calls as G.729.
- **GSM**—The global system for mobile communications (GSM) codec. GSM enables the MNET system for GSM wireless handsets to operate with Cisco Unified CallManager. Assign GSM devices to a device pool that specifies GSM as the audio codec for calls within the GSM region and between other regions. Depending on device capabilities, this includes GSM EFR (enhanced full rate) and GSM FR (full rate).
- **Wideband**—Currently only supported for calls from IP phone to IP phone. The wideband audio codec, uncompressed with a 16-bit, 16-kHz sampling rate, works with phones with handsets, acoustics, speakers, and microphones that can support high-quality audio bandwidth, such as Cisco Unified IP Phone 7900 model phones.

Tip Regions that specify wideband as the codec type must have a large amount of network bandwidth available because wideband uses four times as much bandwidth as G.711.

The total bandwidth that is used per call stream depends on the audio codec type as well as factors such as data packet size and overhead (packet header size), as indicated in Table 5-1. (The bandwidth information provided in Table 5-1 applies to Ethernet.)

Note Each call includes two streams, one in each direction.

Note The codecs specified in Table 5-1 correlate to an approximate bandwidth usage per call. For more information on bandwidth usage for each codec, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)* for the current release of Cisco Unified CallManager.

Table 5-1 Bandwidth Used Per Call by Each Codec Type

Audio Codec	Bandwidth Used for Data Packets Only (Fixed Regardless of Packet Size)	Bandwidth Used Per Call (Including IP Headers) With 30-ms Data Packets	Bandwidth Used Per Call (Including IP Headers) With 20-ms Data Packets
G.711	64 kbps	80 kbps	88 kbps
G.722	24 kbps	80 kbps	88 kbps
G.723	6 kbps	24 kbps	Not applicable
G.729	8 kbps	24 kbps	32 kbps
Wideband[1]	256 kbps	272 kbps	280 kbps
GSM[2]	13 kbps	29 kbps	37 kbps

[1] Uncompressed. Cisco Unified CallManager supports wideband audio from IP phone to IP phone for Cisco Unified IP Phone 7900 Family model phones only.

[2] Global system for mobile communications.

.3.) The phone configuration file strictly requires the IP address (in the a.b.c.d format) of NTP server(s). Do not use hostname of FQDN.

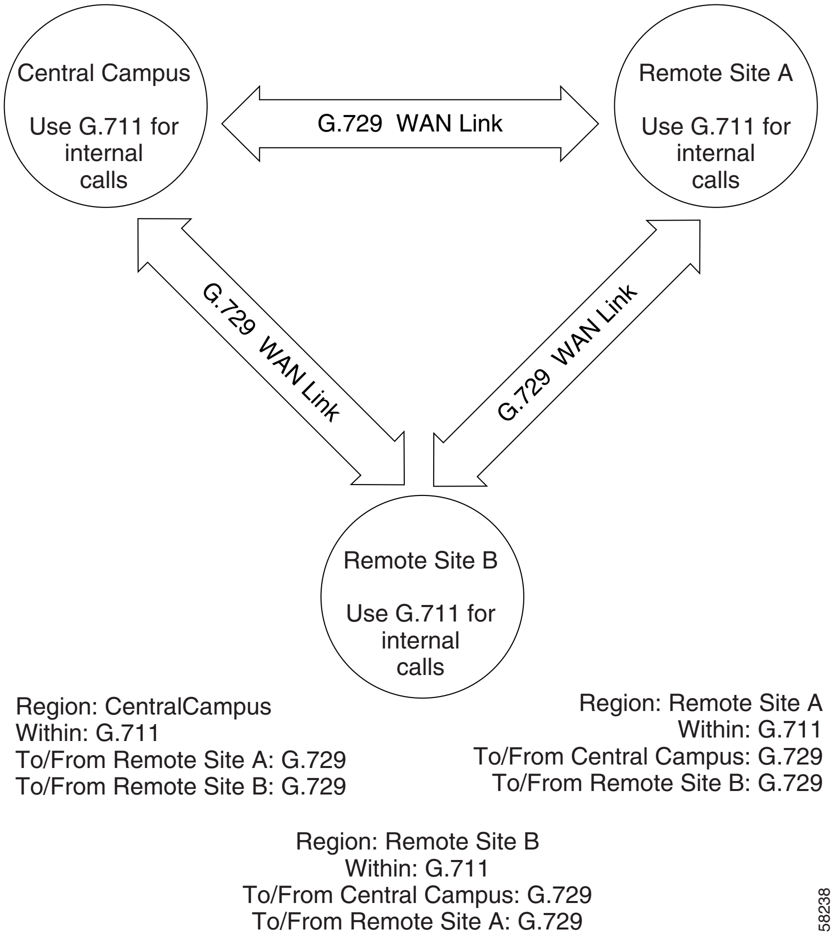
Example

Figure 5-1 shows a very simple region configuration example for deployment with a central site and two remote branches. In the example, an administrator configures a region for each site. The G.711 codec equals the maximum bandwidth codec that is used for calls within each site, and the G.729 codec equals the maximum bandwidth codec that is used for calls between sites across the WAN link.

After region configuration, the administrator assigns devices to the following sites:

- The Central Campus site to device pools that specify CentralCampus as the region setting
- Remote Site A to device pools that specify RemoteSiteA as the region setting
- Remote Site B to device pools that specify RemoteSiteB for the region setting

Figure 5-1 Simple Region Example


Central Campus
Use G.711 for internal calls
G.729 WAN Link
Remote Site A
Use G.711 for internal calls
G.729 WAN Link
G.729 WAN Link
Remote Site B
Use G.711 for internal calls
Region: CentralCampus
Within: G.711
To/From Remote Site A: G.729
To/From Remote Site B: G.729
Region: Remote Site A
Within: G.711
To/From Central Campus: G.729
To/From Remote Site B: G.729
Region: Remote Site B
Within: G.711
To/From Central Campus: G.729
To/From Remote Site A: G.729
58238

Locations and Regions

In Cisco Unified CallManager, locations-based call admission control works in conjunction with regions to define the characteristics of a network link.

- Regions define the type of codec that is used on the link (and therefore, the amount of bandwidth that is used per call).
- Locations define the amount of available bandwidth for the link.

You must assign each device on the network to both a region (by means of a device pool) and a location. See the "Call Admission Control" section on page 5-13.

Deleting a Region

Note You cannot delete a region that any device pools are using.

To find out which device pools use the region, choose **Dependency Records** from the Related Links drop-down list box on the Region Configuration window and click **Go**.

Before deleting a region that is currently in use, you must perform either or both of the following tasks:

- Update the device pools to use a different region.
- Delete the device pools that use the region that you want to delete.

For more information, refer to the *Cisco Unified CallManager Administration Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Device Pools

Device pools provide a convenient way to define a set of common characteristics that can be assigned to devices. You can specify the following device characteristics for a device pool:

- Device Pool Name—Specifies the name for the new device pool.
- Cisco Unified CallManager group—Specifies a prioritized list of up to three Cisco Unified CallManagers to facilitate redundancy. The first Cisco Unified CallManager in the list serves as the primary Cisco Unified CallManager for that group, and the other members of the group serve as secondary (backup) Cisco Unified CallManagers. See the "Cisco Unified CallManager Groups" section on page 5-3 for more details.
- Date/Time group—Specifies the date and time zone for a device. See the "Date/Time Groups" section on page 5-4 for more details.
- Region—Specifies the audio and video codecs that are used within and between regions. Use regions only if you have different types of codecs within the network. See the "Regions" section on page 5-5 for more details.
- Softkey template—Manages the softkeys that are associated with applications on Cisco Unified IP Phones. See the "Softkey Template Configuration" section in the *Cisco Unified CallManager Administration Guide* for more details.
- Survivable Remote Site Telephony (SRST) reference—Specifies the gateway that provides SRST functionality for the devices in a device pool. See the "Survivable Remote Site Telephony References" section on page 5-13 for more details.
- Calling search space for auto-registration (optional)—Specifies the partitions that an auto-registered device can reach when a call is placed. See the "Partitions and Calling Search Spaces" section on page 15-1 for more details.
- Media resource group list (optional)—Specifies a prioritized list of media resource groups. An application chooses 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. See the "Media Resource Group Lists" section on page 22-4 for more details.
- Network hold music on hold (MOH) audio sources (optional)—Specifies the audio source for network hold. See the "Music On Hold Audio Sources" section in the *Cisco Unified CallManager Features and Services Guide* for more details.
- User hold music on hold (MOH) audio source (optional)—Specifies the audio source for user hold. See the "Music On Hold Audio Sources" section in the *Cisco Unified CallManager Features and Services Guide* for more details.
- Network locale—Contains a definition of the tones and cadences that the phones and gateways use in a device pool in a specific geographic area.

Note You must choose only a network locale that is already installed and that the associated devices support. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.

- User locale—Identifies a set of detailed information to support users, including language and font. This characteristic associates with the phones and gateways in a device pool.
- Connection Monitor Duration—Resolves WAN link flapping issues between Cisco Unified CallManager and SRST. See the "Survivable Remote Site Telephony References" section on page 5-13 for more information.
- MLPP Precedence and Preemption Information—Manages MLPP settings:
  - MLPP Indication—Specifies whether devices in the device pool that are capable of playing precedence tones will use the capability when the devices plan an MLPP precedence call.
  - MLPP Preemption—Specifies whether devices in the device pool that are capable of preempting calls in progress will use the capability when the devices plan an MLPP precedence call.
  - MLPP Domain—Specifies a hexadecimal value for the MLPP domain that is associated with the device pool. Device pools refer to the configured MLPP domain.

Note You must configure the preceding items before you configure a device pool if you want to choose the items for the device pool.

After adding a new device pool to the database, you can use it to configure devices such as Cisco Unified IP Phones, gateways, conference bridges, transcoders, media termination points, voice-mail ports, and CTI route points.

If using auto-registration, you can assign all devices of a given type to a device pool by using the Device Defaults window in Cisco Unified CallManager Administration.

For more information, refer to Updating Device Defaults in the *Cisco Unified CallManager Administration Guide*.

Updating Device Pools

If you make changes to a device pool, you must reset the devices in that device pool before the changes will take effect.

You cannot delete a device pool that has been assigned to any devices or one that is used for Device Defaults configuration.

To find out which devices are using the device pool, choose **Dependency Records** from the Related Links drop-down list box on the Device Pool Configuration window and click **Go**.

If you try to delete a device pool that is in use, a message displays. Before deleting a device pool that is currently in use, you must perform either or both of the following tasks:

- Update the devices to assign them to a different device pool.
- Delete the devices that are assigned to the device pool that you want to delete.

LDAP

Cisco Unified CallManager uses the Lightweight Directory Access Protocol (LDAP) directory to store authentication and authorization information about users of Cisco Unified CallManager applications, which interface with Cisco Unified CallManager. Authentication establishes the user right to access the system, while authorization identifies the telephony resources that a user is permitted to use, such as a specific telephone extension.

The LDAP directory provides applications with a standard method for accessing and modifying the information that is stored in the directory. This capability provides the benefit of enabling companies to centralize all user information in a single repository that is available to several applications, thereby reducing maintenance costs through the ease of adds, moves, and changes.

Cisco Unified CallManager provides support for an optional, external LDAP directory. When used, Cisco Unified CallManager and related applications store all application data in a local database instead of in the directory. Cisco Unified CallManager supports integration with the customer directory, and it provides default user authentication with the database as well as user authentication with the customer directory.

To use the LDAP directory with Cisco Unified CallManager, modify information directly from the LDAP server and then configure the following LDAP parameters by using Cisco Unified CallManager Administration.

- LDAP System—Configure this parameter to enable synchronization from the LDAP server. Choose the LDAP server type, such as Microsoft Active Directory (AD) or Netscape LDAP Server, and the LDAP attribute for the user ID.
- LDAP Directory—Use this parameter to find and list LDAP directories and to add information to the LDAP directory, such as LDAP configuration name, LDAP directory synchronization schedule, user fields to be synchronized, and LDAP server information. You must enable synchronization from the LDAP server on the LDAP System window before you can make any changes to this information.
- LDAP Authentication—Configure this parameter to enable LDAP authentication for end users. When the LDAP authentication is turned on, the system authenticates the user's password against the LDAP server instead of the Cisco Unified CallManager database, and it synchronizes the end user information from the LDAP server to the Cisco Unified CallManager database. You must enable synchronization from the LDAP server on the LDAP System window before you can make any changes to this information.

Note You can switch between LDAP parameters by choosing the menu option that you want to configure from the Related Links drop-down list box on the LDAP Configuration windows.

If you want to use your Active Directory or Netscape corporate directory with Cisco Unified CallManager, you must synchronize the directory with the Cisco Unified CallManager database by accessing **System > LDAP > LDAP System**. You set up the directory synchronization agreements by accessing **System > LDAP > LDAP Directory**.

You must activate the Cisco DirSync service from Cisco Unified CallManager Serviceability to synchronize the AD/Netscape directories. The Cisco DirSync service interacts with these directories by synchronizing the data, reading the customer directory information, and updating the Cisco Unified CallManager database.

To activate Cisco DirSync, access **Control Center > Feature Services** and navigate to Directory Services.

- Set up the directory synchronization agreements by accessing **System > LDAP > LDAP Directory**.
- Set up the configuration used by Cisco DirSync by accessing **System > LDAP > LDAP System** and **System > LDAP > LDAP Directory.**

See "Understanding the Directory" for more information about using directories with Cisco Unified CallManager.

Call Admission Control

Use call admission control to maintain a desired level of voice quality over a WAN link. For example, you can use call admission control to regulate the voice quality on a 56-kbps frame relay line that connects your main campus and a remote site.

Voice quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call admission control regulates voice quality by limiting the number of calls that can be active at the same time on a particular link. Call admission control does not guarantee a particular level of audio quality on the link, but it does allow you to regulate the amount of bandwidth that active calls on the link consume.

Cisco Unified CallManager supports two types of call admission control:

- Locations—Use locations to implement call admission control in a centralized call-processing system. Call admission control lets you regulate voice quality by limiting the amount of bandwidth that is available for calls over links between the locations.
- H.323 Gatekeeper—Use an H.323 gatekeeper, also known as a Cisco Multimedia Conference Manager (MCM), to provide call admission control in a distributed system with a separate Cisco Unified CallManager or Cisco Unified CallManager cluster at each site.

Note If you do not use call admission control to limit the voice bandwidth on an IP WAN link, the system allows an unlimited number of calls to be active on that link at the same time. This can cause the voice quality of each call to degrade as the link becomes oversubscribed.

See the "Call Admission Control" section on page 8-1 for more information.

Survivable Remote Site Telephony References

Survivable Remote Site Telephony (SRST) gets used at sites that depend on a centralized Cisco Unified CallManager cluster that is accessible via a WAN connection. SRST provides telephony service to IP phones at the remote site in the event of a WAN outage. An SRST-enabled router has features that allow calls between IP phones at the remote site to call each other, allow calls from the PSTN to reach the IP phones, and allow calls from the IP phones to reach the external world through the PSTN. Intelligence in the SRST router that can accept registrations from the IP phones and route calls based on the directory numbers that are registered, and based on the routing that is configured for the PSTN link, accomplishes that.

Survivable remote site telephony (SRST) references, a configurable option in Cisco Unified CallManager Administration, provide limited call capability in the event of a WAN outage. Using SRST references, IP gateways can take over limited Cisco Unified CallManager functionality. When phones lose connectivity to all associated Cisco Unified CallManagers, the phones in a device pool attempt to make a Cisco Unified CallManager connection to the SRST reference IP gateway.

The status line indication on the IP phone that shows the phone has failed over to the backup proxy (SRST gateway) provides the only user interactions with SRST.

Device Pool Settings for SRST

The system administrator can configure the SRST configuration for a device pool of phones. The following list gives Device Pool configuration options that are available:

- Disable–If a phone cannot reach any Cisco Unified CallManagers, it does not try to connect to an SRST gateway.
- Use Default Gateway–If a phone cannot reach any Cisco Unified CallManagers, it tries to connect to its IP gateway as an SRST gateway.
- User-defined–If a phone cannot reach any Cisco Unified CallManagers, it tries to connect to an administrator-specified SRST gateway. The SRST Reference field of the Device Pool Configuration lists user-defined SRST references.

The administrator defines SRST configurations in the SRST Reference Configuration window. Any preceding SRST configuration option can apply to a device pool. The Cisco TFTP reads the SRST configuration and provides it to the IP phone in a .cnf.xml file. The IP phone reacts appropriately to the SRST configuration.

Connection Monitor Duration

An IP phone that connect to the SRST over a Wide Area Network (WAN) reconnects itself to Cisco Unified CallManager as soon as it can establish a connection with Cisco Unified CallManager over the WAN link. However, if the WAN link is unstable, the IP phone switches back and forth between the SRST and Cisco Unified CallManager. This situation causes temporary loss of phone service (no dial tone). These reconnect attempts, known as WAN link flapping issues, continue until the IP phone successfully reconnects itself to Cisco Unified CallManager. These WAN link disruptions fit into two classifications: infrequent random outages that occur on an otherwise stable WAN and the sporadic, frequent disruptions that last a few minutes.

To resolve the WAN link flapping issues between Cisco Unified CallManager and SRST, Cisco Unified CallManager provides an enterprise parameter and a setting in the Device Pool Configuration window that is called Connection Monitor Duration. Depending upon system requirements, the administrator decides which parameter to use. The value of the parameter gets delivered to the IP phone in the XML configuration file.

- The default for the enterprise parameter specifies 120 seconds. Use the enterprise parameter to change the connection duration monitor value for all IP phones in the Cisco Unified CallManager cluster.
- Use the Device Pool Configuration window to change the connection duration monitor value for all IP phones in a specific device pool.

SRST Reference Configuration Options for SIP Phones

A remote site may have a mix of SCCP and SIP endpoints in addition to PSTN gateway access. For calls to be routed between the different protocols and the PSTN, three different features will be configured in one SRST router that will allow calls to be routed between SCCP phones, SIP phones, and the PSTN during a WAN outage. In addition, the SRST Reference Configuration window in Cisco Unified CallManager Administration provides two fields:

- SIP Network/IP Address—The SIP network/IP address applies for SIP SRST. This address notifies the SIP phone where to send SIP Register message for SIP SRST.
- SIP Port—SIP port of the SRST gateway. Default specifies 5060.

For more information, refer to "SRST Reference Configuration Settings" in the *Cisco Unified CallManager Administration Guide*.

For information about configuring security for the SRST reference and the SRST-enabled gateway, refer to *Cisco Unified CallManager Security Guide*.

MLPP Domain

Because the MLPP service applies to a domain, Cisco Unified CallManager only marks a precedence level to connections and resources that belong to calls from MLPP users in a given 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.

To define an MLPP domain, configure the following MLPP domain information:

- Domain Name—Name of the MLPP domain.
- Domain Identifier—Configure the MLPP domain identifier as a hexadecimal value of zero or greater (the default value specifies zero).

The MLPP domain identifier comprises the collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber (who belongs to a particular domain) places a precedence call to another MLPP subscriber (who belongs to the same domain), the MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. The MLPP service availability does not cross domains. Device pools refer to the configured MLPP domain.

Note You must reset all devices for a change to this setting to take effect.

Enterprise Parameters

Enterprise parameters provide default settings that apply to all devices and services in the same cluster. When you install a new Cisco Unified CallManager, it uses the enterprise parameters to set the initial values of its device defaults.

You cannot add or delete enterprise parameters, but you can update existing enterprise parameters. Cisco Unified CallManager Administration segments enterprise parameters by categories; for example, CCMAdmin parameters, CCMUser parameters, and CDR parameters.

You can display additional descriptions for enterprise parameters by using the question mark button on the Enterprise Parameters Configuration window.

Service Parameters

Service parameters for Cisco Unified CallManager allow you to configure different services on selected servers. You can view a list of parameters and their descriptions by clicking the question mark button that displays on the Service Parameters Configuration window. You can view the list with a particular parameter at the top by clicking that parameter.

If you deactivate a service by using Cisco Unified CallManager Serviceability, Cisco Unified CallManager retains any updated service parameter values. If you start the service again, Cisco Unified CallManager sets the service parameters to the changed values.

Caution Some changes to service parameters may cause system failure. Cisco recommends that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) requests that you make changes.

Dependency Records

To find specific information about system-level settings such as servers, device pools, and date/time groups, choose **Dependency Records** from the Related Links drop-down list box on the Cisco Unified CallManager Administration configuration windows for each system-level setting and click **Go**.

If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Note You cannot view Dependency Records from the Device Defaults and Enterprise Parameters Configuration windows.

The Cisco Unified CallManager Configuration Dependency Records window provides information about Cisco Unified CallManager groups that it accesses. The Date/Time Group Configuration Dependency Records window provides information about Device Pools that it accesses.

For more information about Dependency Records, refer to Accessing Dependency Records, *Cisco Unified CallManager Administration Guide*.

System Configuration Checklist

Table 5-2 lists the general steps for configuring system-level settings.

Table 5-2 System Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Configure the server to specify the address of the server where Cisco Unified CallManager is installed.	Server Configuration, page 5-1 Server Configuration, *Cisco Unified CallManager Administration Guide*
Step 2	Specify the ports and other properties for each Cisco Unified CallManager that is installed in the same cluster.	Cisco Unified CallManager Configuration, page 5-2 Cisco Unified CallManager Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Configure Cisco Unified CallManager groups for redundancy.	Cisco Unified CallManager Groups, page 5-3 Redundancy, page 7-1 Cisco Unified CallManager Group Configuration, *Cisco Unified CallManager Administration Guide*
Step 4	Configure phone NTP references, so SIP phones can get the date and time from the NTP server (optional).	Phone NTP Reference Configuration for SIP Phones, page 5-4 Phone NTP Reference Configuration, *Cisco Unified CallManager Administration Guide*
Step 5	Configure Date/Time groups to define time zones for the various devices that are connected to Cisco Unified CallManager.	Date/Time Groups, page 5-4 Date/Time Group Configuration, *Cisco Unified CallManager Administration Guide*
Step 6	Configure regions to specify the codec that can be used for calls between devices within that region, and between that region and other regions, if needed. **Tip** You do not need to configure regions if you are using only the default G.711 audio codec.	Regions, page 5-5 Region Configuration, *Cisco Unified CallManager Administration Guide*
Step 7	Configure device pools to define a set of common characteristics that can be assigned to devices.	Device Pools, page 5-10 Device Pool Configuration, *Cisco Unified CallManager Administration Guide*
Step 8	Configure media resource groups and media resource group lists.	Media Resource Management, page 22-1 Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide*

Table 5-2 System Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 9	Configure LDAP to store authentication and authorization information about users who interface with Cisco Unified CallManager.	LDAP, page 5-12 Understanding the Directory
Step 10	Configure locations or gatekeepers for call admission control.	Locations and Regions, page 5-9 Call Admission Control, page 8-1
Step 11	Configure survivable remote site telephony (SRST) references to preserve rudimentary call capability.	Survivable Remote Site Telephony References, page 5-13 Survivable Remote Site Telephony Configuration, *Cisco Unified CallManager Administration Guide*
Step 12	Configure the MLPP domain.	MLPP Domain, page 5-15 Multilevel Precedence and Preemption, *Cisco Unified CallManager Features and Services Guide*
Step 13	Update enterprise parameters, if necessary.	Enterprise Parameters, page 5-15 Enterprise Parameters Configuration, *Cisco Unified CallManager Administration Guide*
Step 14	Update service parameters, if necessary. For example, configure the DRF backup and restore master agent in the Cisco Unified CallManager Administration Service Parameters Configuration window.	Service Parameters, page 5-16 Dependency Records, page 5-16 Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topics

- Server Configuration, page 5-1
- Cisco Unified CallManager Configuration, page 5-2
- Cisco Unified CallManager Groups, page 5-3
- Date/Time Groups, page 5-4
- Regions, page 5-5
- Device Pools, page 5-10
- LDAP, page 5-12
- Call Admission Control, page 5-13
- Survivable Remote Site Telephony References, page 5-13
- MLPP Domain, page 5-15
- Enterprise Parameters, page 5-15

- Service Parameters, page 5-16
- Dependency Records, page 5-16
- Redundancy, page 7-1

Additional Cisco Documentation

- *Cisco Unified CallManager Administration Guide*

Clustering

The clustering feature of Cisco Unified CallManager provides a mechanism for seamlessly distributing call processing across the infrastructure of a converged IP network. Clustering provides transparent sharing of resources and features and enables system scalability.

This section covers the following topics:

- Clusters, page 6-1
- Balanced Call Processing, page 6-3
- Where to Find More Information, page 6-4

Clusters

A cluster comprises a set of Cisco Unified CallManager servers that share the same database and resources. You can configure the servers in a cluster in various ways to perform the following functions:

- Database server (only one database server in the cluster)
- TFTP server
- Application software server

Before you install the Cisco Unified CallManager software on subsequent servers, you must define the nodes in Server Configuration in Cisco Unified CallManager Administration.

Using the Service Activation window in the Cisco Unified CallManager Serviceability application, you can specify which server performs which function for the cluster. You can dedicate a particular server to one function or combine several functions on one server, depending on the size of your system and the level of redundancy that you want.

Each cluster can have only one database server (first node) and usually one TFTP server (either separate or combined).

Tip In a very large cluster, simultaneous initialization, the process that occurs after a Cisco Unified CallManager failure, can cause an overload of the database server. To limit the number of Cisco Unified CallManager services that will simultaneously initialize, you can configure the “Max Simultaneous Cisco CallManager Initializations” service parameter. This parameter defaults to 0 and, with this value, the number of Cisco Unified CallManager services that can initialize simultaneously is unlimited. Any non-zero value will limit the number of services to that specific value.

Tip Another service parameter that should be configured is the “Restart Cisco CallManager on Initialization Exception” parameter. This parameter determines whether the Cisco CallManager service restarts if an error occurs during initialization. This parameter defaults to TRUE and, with this value, the Cisco CallManager initialization will abort when an error occurs during initialization. Setting the value to FALSE allows initialization to continue when an error is encountered. These parameters are clusterwide and can be located in the System - General subsection. Refer to “Service Parameters Configuration” in the *Cisco Unified CallManager Administration Guide* for detailed information on configuring service parameters.

For details on cluster size and recommended configurations, refer to the *Cisco Unified Communications Solution Reference Network Design Guide*.

For details of the Service Activation window, refer to the *Cisco Unified CallManager Serviceability System Guide* and to the *Cisco Unified CallManager Serviceability Administration Guide*.

Intercluster Communication

In very large systems, you might have to configure more than one cluster to handle the call-processing load. Communication between the clusters occurs by means of intercluster trunks. Most large systems use one of two main types of multicluster configurations:

- Large, single campus, or metropolitan-area network (MAN)
- Multisite WAN with distributed call processing (one or more Cisco Unified CallManagers at each site)

Because intercluster trunks in a MAN usually have sufficient bandwidth, they do not require any call admission control mechanism. Multisite WANs with distributed call processing typically use gatekeeper technology for call admission control.

Intracluster Communication

Cisco Unified CallManager also supports intracluster communication, which is a multisite WAN with centralized call processing (no Cisco Unified CallManager at the remote site or sites). Multisite WANs with centralized call processing use the locations feature in Cisco Unified CallManager to implement call admission control.

Most features of Cisco Unified CallManager do not extend beyond a single cluster, but the following features do exist between clusters:

- Basic call setup
- G.711 and G.729 calls
- Multiparty conference
- Call hold
- Call transfer
- Call park
- Calling line ID

For more information about intercluster communication and call admission control, refer to the *Cisco Unified Communications Solution Reference Network Design Guide.*

Balanced Call Processing

After installing the Cisco Unified CallManagers that form a cluster, you can balance the call-processing load across the system by distributing the devices (such as phones and gateways) among the various Cisco Unified CallManagers in the cluster. To distribute the devices, you configure Cisco Unified CallManager groups and device pools and then assign the devices to the device pools in a way that achieves the type of load balancing that you want.

Cisco Unified CallManager groups and device pools represent logical groupings of devices that you can arrange in any way that you want. For ease of administration, make sure that all the devices in a group or pool share a common and easily identified characteristic, such as their physical location on the network.

You can also use Cisco Unified CallManager groups to establish redundancy (backup call processors) for the primary Cisco Unified CallManager in the group. A Cisco Unified CallManager group comprises an ordered list of up to three Cisco Unified CallManager servers. During normal operation, the first (primary) Cisco Unified CallManager in the group controls all device pools and devices that are assigned to that group. If the primary Cisco Unified CallManager in a group fails, control of the device pools and devices that are registered with the primary Cisco Unified CallManager transfers to the next Cisco Unified CallManager in the group list.

For example, assume a simplified system that comprises three Cisco Unified CallManagers in a cluster, with 300 existing Cisco Unified IP Phones and provisions to auto-register new phones as they are added later.

- The configuration includes four Cisco Unified CallManager groups: group G1 assigned to device pool DP1, group G2 assigned to device pool DP2, group G3 assigned to device pool DP3, and group G4 assigned to device pool DP4. Group G4 serves as the default group for devices that auto-register.
- Unified CM1 serves as the primary Cisco Unified CallManager for the devices in DP1 and DP2, first backup for DP3, and second backup for the devices in DP4.
- Unified CM2 serves as the primary Cisco Unified CallManager for the devices in DP3 and DP4, first backup for DP1, and second backup for the devices in DP4.
- Unified CM3 serves as the first backup Cisco Unified CallManager for the devices in DP2 and DP4 and second backup for the devices in DP1 and DP3.

Table 6-1 provides an overview of the steps that are required to install and configure a Cisco Unified CallManager cluster.

Table 6-1 Cluster Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Install the database server (first node).	Refer to the installation documentation for the hardware components that you are installing.
Step 2	Gather the information that you need to install Cisco Unified CallManager and any other software applications on the first node and subsequent servers. Also, determine how you will allocate the servers in the cluster.	*Cisco Unified Communications Solution Reference Network Design Guide* *Installing Cisco Unified CallManager Release 5.0(4)* *Cisco Unified IP-IVR Installation Guide*

Table 6-1 Cluster Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 3	Install Cisco Unified CallManager and any additional software applications on the subsequent servers. **Note** Before installing the subsequent servers, you must define the nodes in Server Configuration in Cisco Unified CallManager Administration.	*Installing Cisco Unified CallManager Release 5.0(4)* *Cisco Unified IP-IVR Installation Guide* Server Configuration, *Cisco Unified CallManager Administration Guide*
Step 4	Configure device pools and use them to assign specific devices to a Cisco Unified CallManager group.	Device Pool Configuration, *Cisco Unified CallManager Administration Guide*
Step 5	If you are using an intercluster trunk, install and configure it as an intercluster trunk, either gatekeeper-controlled or non-gatekeeper-controlled.	*Cisco Unified Communications Solution Reference Network Design Guide* Configuring a Trunk, *Cisco Unified CallManager Administration Guide* Trunk Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 6	If you want to provide call admission control for an intercluster trunk, configure either a gatekeeper-controlled intercluster trunk or Cisco Unified CallManager locations.	*Cisco Unified Communications Solution Reference Network Design Guide* Trunk Configuration, *Cisco Unified CallManager Administration Guide* Location Configuration, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topics

- Cisco Unified CallManager Group Configuration, *Cisco Unified CallManager Administration Guide*
- Device Pool Configuration, *Cisco Unified CallManager Administration Guide*
- Trunk Configuration, *Cisco Unified CallManager Administration Guide*
- Location Configuration, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design Guide*
- *Installing Cisco Unified CallManager Release 5.0(4)*
- *Cisco Unified IP-IVR Installation Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*

CHAPTER 7

Redundancy

Cisco Unified CallManager provides several forms of redundancy:

- Call-processing redundancy—Using Cisco Unified CallManager groups, you can designate backup Cisco Unified CallManagers to handle call processing for a disabled Cisco Unified CallManager in a form of redundancy known as device failover.
- Media resource redundancy
- CTI redundancy

This section covers the following topics:

- Cisco Unified CallManager Redundancy Groups, page 7-1
- Media Resource Redundancy, page 7-4
- CTI Redundancy, page 7-4
- Where to Find More Information, page 7-4

Cisco Unified CallManager Redundancy Groups

Groups and clusters form logical collections of Cisco Unified CallManagers and their associated devices. Groups and clusters do not necessarily relate to the physical locations of any of their members.

A cluster comprises a set of Cisco Unified CallManagers that share a common database. When you install and configure the Cisco Unified CallManager software, you specify which servers and which Cisco Unified CallManagers belong to the same cluster.

A group comprises a prioritized list of up to three Cisco Unified CallManagers. You can associate each group with one or more device pools to provide call-processing redundancy. You use Cisco Unified CallManager Administration to define the groups, to specify which Cisco Unified CallManagers belong to each group, and to assign a Cisco Unified CallManager group to each device pool.

Cisco Unified CallManager Groups

A Cisco Unified CallManager group comprises a prioritized list of up to three Cisco Unified CallManagers. Each group must contain a primary Cisco Unified CallManager, and it may contain one or two backup Cisco Unified CallManagers. The order in which you list the Cisco Unified CallManagers in a group determines the priority order.

Cisco Unified CallManager groups provide both redundancy and recovery:

- *Failover*—Occurs when the primary Cisco Unified CallManager in a group fails, and the devices reregister with the backup Cisco Unified CallManager in that group.
- *Fallback*—Occurs when a failed primary Cisco Unified CallManager comes back into service, and the devices in that group reregister with the primary Cisco Unified CallManager.

Under normal operation, the primary Cisco Unified CallManager in a group controls call processing for all the registered devices (such as phones and gateways) that are associated with that group.

If the primary Cisco Unified CallManager fails for any reason, the first backup Cisco Unified CallManager in the group takes control of the devices that were registered with the primary Cisco Unified CallManager. If you specify a second backup Cisco Unified CallManager for the group, it takes control of the devices if both the primary and the first backup Cisco Unified CallManagers fail.

When a failed primary Cisco Unified CallManager comes back into service, it takes control of the group again, and the devices in that group automatically reregister with the primary Cisco Unified CallManager.

You associate devices with a Cisco Unified CallManager group by using device pools. You can assign each device to one device pool and associate each device pool with one Cisco Unified CallManager group. You can combine the groups and device pools in various ways to achieve the desired level of redundancy. For example, Figure 7-1 shows a simple system with three Cisco Unified CallManagers in a single group that is controlling 800 devices.

Figure 7-1 Cisco Unified CallManager Group

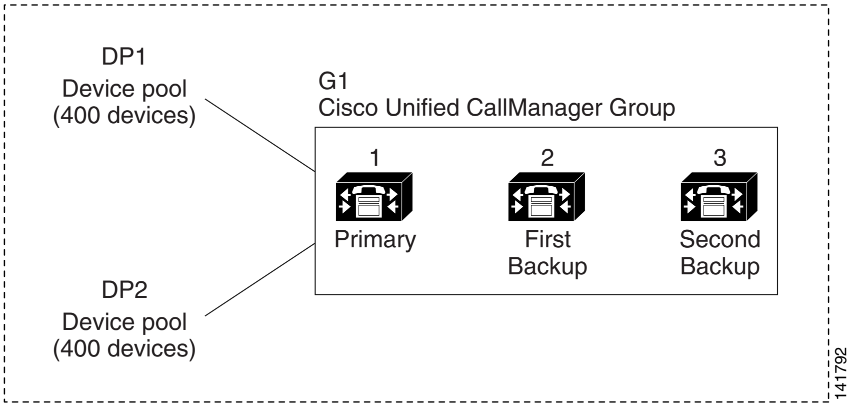


Figure 7-1 depicts Cisco Unified CallManager group G1 that is assigned with two device pools, DP1 and DP2. Cisco Unified CallManager 1, as the primary Cisco Unified CallManager in group G1, controls all 800 devices in DP1 and DP2 under normal operation. If Cisco Unified CallManager 1 fails, control of all 800 devices transfers to Cisco Unified CallManager 2. If Cisco Unified CallManager 2 also fails, control of all 800 devices transfers to Cisco Unified CallManager 3.

The configuration in Figure 7-1 provides call-processing redundancy, but it does not distribute the call-processing load very well among the three Cisco Unified CallManagers in the example. For information on load balancing, see the "Distributing Devices for Redundancy and Load Balancing" section on page 7-3.

Note Empty Cisco Unified CallManager groups will not function.

Distributing Devices for Redundancy and Load Balancing

Cisco Unified CallManager groups provide both call-processing redundancy and distributed call processing. How you distribute devices, device pools, and Cisco Unified CallManagers among the groups determines the level of redundancy and load balancing in your system.

In most cases, you would want to distribute the devices in a way that prevents the other Cisco Unified CallManagers from becoming overloaded if one Cisco Unified CallManager in the group fails. Figure 7-2 shows one possible way to configure the Cisco Unified CallManager groups and device pools to achieve both distributed call processing and redundancy for a system of three Cisco Unified CallManagers and 800 devices.

Figure 7-2 Redundancy Combined with Distributed Call Processing

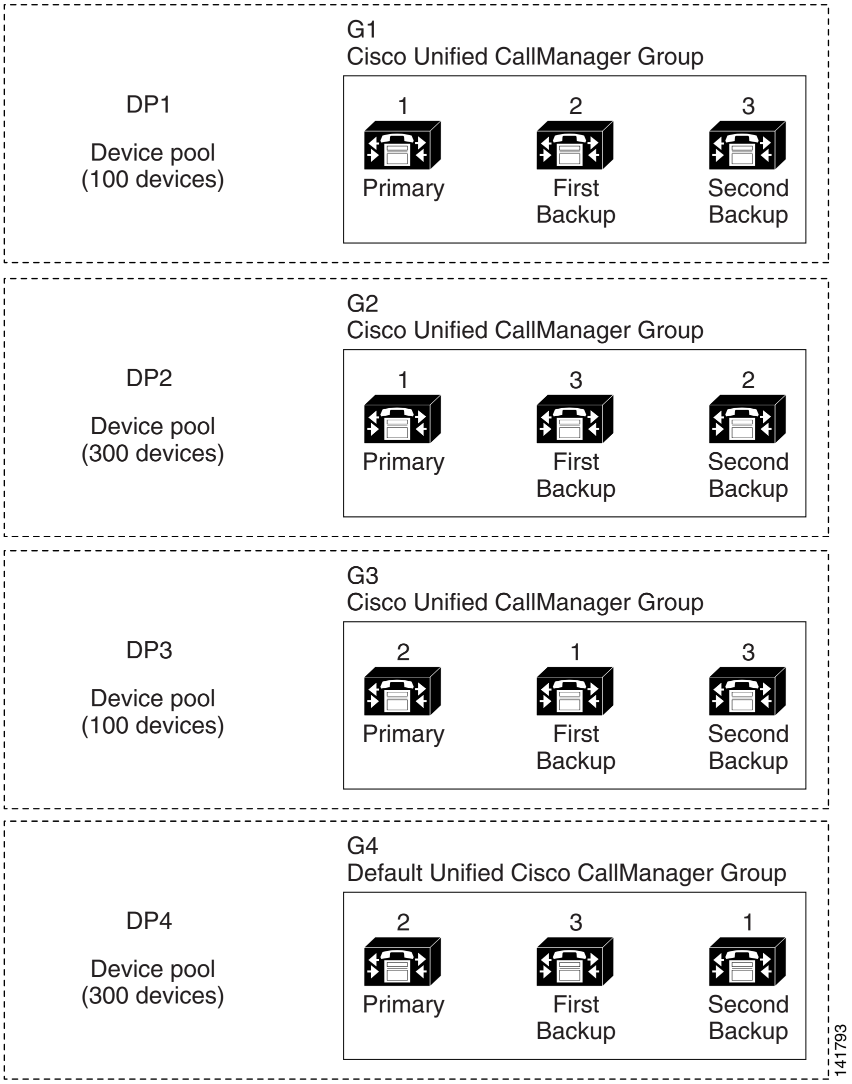


Figure 7-2 depicts the Cisco Unified CallManager groups as they are configured and assigned to device pools, so Cisco Unified CallManager 1 serves as the primary controller in two groups, G1 and G2. If Cisco Unified CallManager 1 fails, the 100 devices in device pool DP1 reregister with Cisco Unified CallManager 2, and the 300 devices in DP2 reregister with Cisco Unified CallManager 3.

Similarly, Cisco Unified CallManager 2 serves as the primary controller of groups G3 and G4. If Cisco Unified CallManager 2 fails, the 100 devices in DP3 reregister with Cisco Unified CallManager 1, and the 300 devices in DP4 reregister with Cisco Unified CallManager 3. If Cisco Unified CallManager 1 and Cisco Unified CallManager 2 both fail, all devices reregister with Cisco Unified CallManager 3.

For more information on distributed call processing, see the "Balanced Call Processing" section on page 6-3.

Media Resource Redundancy

Media resource lists provide media resource redundancy by specifying a prioritized list of media resource groups. An application can select required media resources from among the available ones according to the priority order that is defined in the media resource list. For more information on media resource redundancy, see the "Media Resource Management" section on page 22-1.

CTI Redundancy

Computer telephony integration (CTI) provides an interface between computer-based applications and telephony functions. CTI uses various redundancy mechanisms to provide recovery from failures in any of the following major components:

- Cisco Unified CallManager
- Cisco CTIManager
- Applications that use CTI

CTI uses Cisco Unified CallManager redundancy groups to provide recovery from Cisco Unified CallManager failures. To handle recovery from failures in Cisco CTIManager itself, CTI allows you to specify primary and backup Cisco CTIManagers for the applications that use CTI. Finally, if an application fails, the Cisco CTIManager can redirect calls that are intended for that application to a forwarding directory number.

Where to Find More Information

Related Topics

- Clustering, page 6-1
- Media Resource Management, page 22-1

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design (SRND)*

CHAPTER 8

Call Admission Control

Call admission control enables you to control the audio quality and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time. For example, you can use call admission control to regulate the voice quality on a 56-kbps frame relay line that connects your main campus and a remote site.

Audio and video quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call admission control regulates audio and video quality by limiting the number of calls that can be active on a particular link at the same time. Call admission control does not guarantee a particular level of audio or video quality on the link, but it does allow you to regulate the amount of bandwidth that active calls on the link consume.

Call admission control operates by rejecting a call for bandwidth and policy reasons. When a call gets rejected due to call admission control, the phone of the called party does not ring, and the caller receives a busy tone. The caller also receives a message on their phone, such as “Not enough bandwidth.”

Without call admission control, customers may perceive that IP voice is low in quality and unreliable. With call admission control, customers experience situations similar to the time-division multiplexing (TDM) processing and realize that they need more bandwidth for peak hours.

This section describes two types of call admission control that you can use with Cisco Unified CallManager:

- Locations, page 8-2, for systems with centralized call processing
- Gatekeepers and Trunks, page 8-6, for systems with distributed call processing

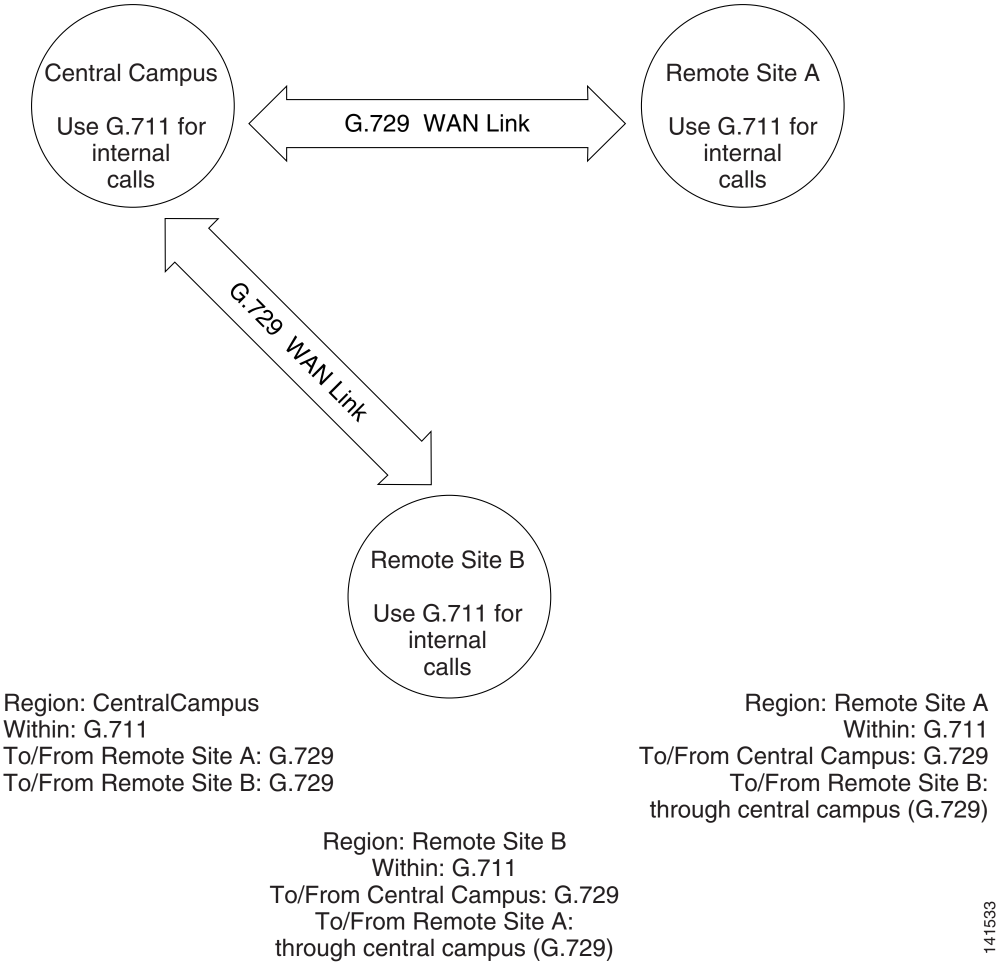
You can choose either of these two methods of call admission control, but you cannot combine them in the same Cisco Unified CallManager system. If your system does not contain IP WAN links with limited available bandwidth, you do not have to use call admission control.

Cisco Unified CallManager also supports Resource Reservation Protocol (RSVP), an additional CAC mechanism that offers additional capabilities for full-mesh network topologies and for large clusters. See “Resource Reservation Protocol” for a description of RSVP.

Locations

The locations feature, available in Cisco Unified CallManager, provides call admission control for centralized call-processing systems. A centralized system uses a single Cisco Unified CallManager cluster to control all the locations. Figure 8-1 illustrates call admission control that is using locations. For more information, refer to the "Location Configuration" section in the *Cisco Unified CallManager Administration Guide* and to the *Cisco Unified Communications Solution Reference Network Design for* Cisco Unified CallManager. For non-centralized systems, Cisco Unified CallManager offers an alternative CAC method, Resource Reservation Protocol (RSVP). See "Resource Reservation Protocol" for a description of RSVP.

Figure 8-1 Call Admission Control Using Locations in a Centralized System


Central Campus
Use G.711 for internal calls
G.729 WAN Link
Remote Site A
Use G.711 for internal calls
G.729 WAN Link
Remote Site B
Use G.711 for internal calls
Region: CentralCampus
Within: G.711
To/From Remote Site A: G.729
To/From Remote Site B: G.729
Region: Remote Site A
Within: G.711
To/From Central Campus: G.729
To/From Remote Site B:
through central campus (G.729)
Region: Remote Site B
Within: G.711
To/From Central Campus: G.729
To/From Remote Site A:
through central campus (G.729)
141533

In a centralized call-processing system, as illustrated in Figure 8-1, the Cisco Unified CallManager cluster resides at the main location, along with other devices such as phones and gateways. The remote locations (for example, branch offices of your company) house additional phones and other devices, but they do not contain any call-processing capability. The remote locations connect to the main location by means of IP WAN links (and possibly PSTN and ISDN links as backups) and to each other by going through the main location (central campus).

Calls between devices at the same location do not need call admission control because those devices reside on the same LAN, which has unlimited available bandwidth. However, calls between devices at different locations must travel over an IP WAN link, which has limited available bandwidth.

The locations feature in Cisco Unified CallManager lets you specify the maximum amount of audio bandwidth (for audio calls) and video bandwidth (for video calls) that is available for calls to and from each location, which thereby limits the number of active calls and limits oversubscription of the bandwidth on the IP WAN links.

Note Each audio call includes two streams, one in each direction. Video calls have four or six streams (that is, two or three streams in each direction).

For example, assume that you have configured the following locations in Cisco Unified CallManager Administration:

Location	Bandwidth (kbps)
San Francisco (main location)	Unlimited
Austin (remote location)	160
Dallas (remote location)	200

Cisco Unified CallManager continues to admit new calls to a link as long as sufficient bandwidth is still available. Thus, if the link to the Austin location in the example has 160 kbps of available bandwidth, that link can support one G.711 call at 80 kbps (in each direction), three G.723 or G.729 calls at 24 kbps each (in each direction), or two GSM calls at 29 kbps each (in each direction). If any additional calls try to exceed the bandwidth limit, the system rejects them, the calling party receives reorder tone, and a text message displays on the phone.

When you configure a location in Cisco Unified CallManager Administration, you assign it a name and maximum audio bandwidth. If you set the audio or video bandwidth to *Unlimited*, you allocate unlimited available bandwidth and allow an unlimited number of active calls on the IP WAN link for that location. In configuring a location, you also assign a video bandwidth for the location. If you set the video bandwidth setting to *None*, no video calls can connect between this location and other locations, but they can take place within this location.

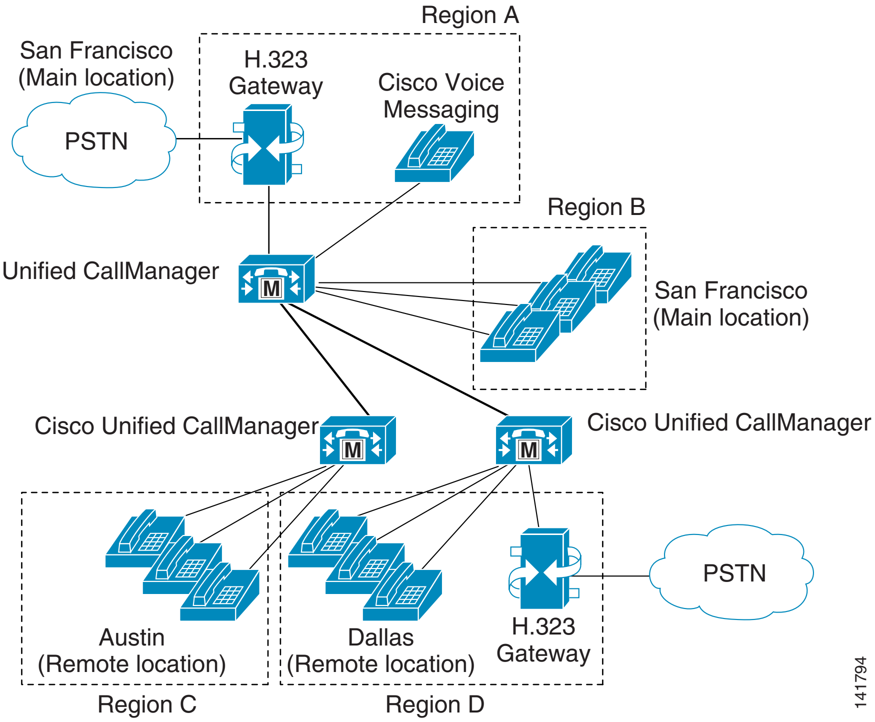
When you configure a phone or other device in Cisco Unified CallManager Administration, you can assign it to a location. If you set the location to *Hub_None*, you assign that device to an unnamed location with unlimited available bandwidth and allow an unlimited number of active calls to and from that device.

Location reservations move to reflect the type of call. When a call changes from video to audio-only, the location reservation moves from the video location to an audio location. Calls that change from audio-only to video cause the opposite change of location reservation.

Locations and Regions

Locations work in conjunction with regions to define the characteristics of a network link. Regions define the type of compression (G.711, G.722, G.723, G.729, GSM, or wideband) that is used on the link, and locations define the amount of available bandwidth for the link. You assign each device in the system to both a region (by means of a device pool) and a location. As illustrated in Figure 8-2, the regions and locations can overlap and intersect in various ways, depending on how you define them. For more information, see the "Regions" section on page 5-5.

Figure 8-2 Interaction Among Locations and Regions



Bandwidth Calculations

In performing location bandwidth calculations for purposes of call admission control, Cisco Unified CallManager assumes that each call stream consumes the following amount of bandwidth:

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

Note Each audio call comprises two call streams. Actual bandwidth consumption per call varies, depending on factors such as data packet size. Cisco Unified CallManager uses these fixed values to simplify the bandwidth calculations for purposes of the locations feature only.

Each video call can comprise four or six call streams. For a video call, total bandwidth represents the sum of the call audio bandwidth plus video bandwidth but does not include the call overhead.

The audio bandwidth value that is specified for a location includes overhead, whereas the video bandwidth value that is specified for a location does not include overhead. For a location, the bandwidth that is available for video calls represents the sum of the audio bandwidth and the video bandwidth. Refer to the "Understanding Video Telephony" chapter for more details.

Cisco Unified CallManager allows calls to complete over a link until sufficient bandwidth does not exist for a new call. At that point, any additional calls fail, and the calling party receives reorder tone.

When a link to a location experiences blockage, it may result from bandwidth leakage that has reduced the usable bandwidth for the location. You can resynchronize the bandwidth allotment to the maximum setting for the location without restarting the Cisco Unified CallManager server. For instructions, refer to "Resynchronizing a Location Bandwidth" in the *Cisco Unified CallManager Administration Guide.*

Note If you resynchronize the bandwidth for a location when calls are using the link, the bandwidth might be oversubscribed until all calls that are using the link disconnect. An oversubscribed link can cause audio and video quality to degrade. For this reason, resynchronize the location bandwidth during hours when the link has low traffic.

Media Termination Point and transcoder represent exceptions to the bandwidth rules that are outlined in the preceding paragraph. Calls that are made through an MTP can complete even if they exceed the available bandwidth limit. Calls that are made through an MTP, however, cannot provide video.

Caution In the United States and Canada, routing an emergency 911 call to a link that has no more available bandwidth can block the 911 call. For each location on your network, always route 911 calls to the local public switched telephone network (PSTN) through a local VoIP gateway.

Location-Based MLPP

Cisco Unified CallManager supports MLPP on Skinny Client Control Protocol phones and TDM (PRI/CAS) trunks. Cisco Unified CallManager also supports MLPP on wide-area network (WAN) links. Location-based call admission control (CAC) manages WAN link bandwidth in Cisco Unified 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 Unified 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.

For more information, see Multilevel Precedence and Preemption in the *Cisco Unified CallManager Features and Services Guide*.

Locations Configuration Checklist

Table 8-1 lists the general steps for configuring call admission control on the basis of locations.

Table 8-1 Locations Configuration Checklist

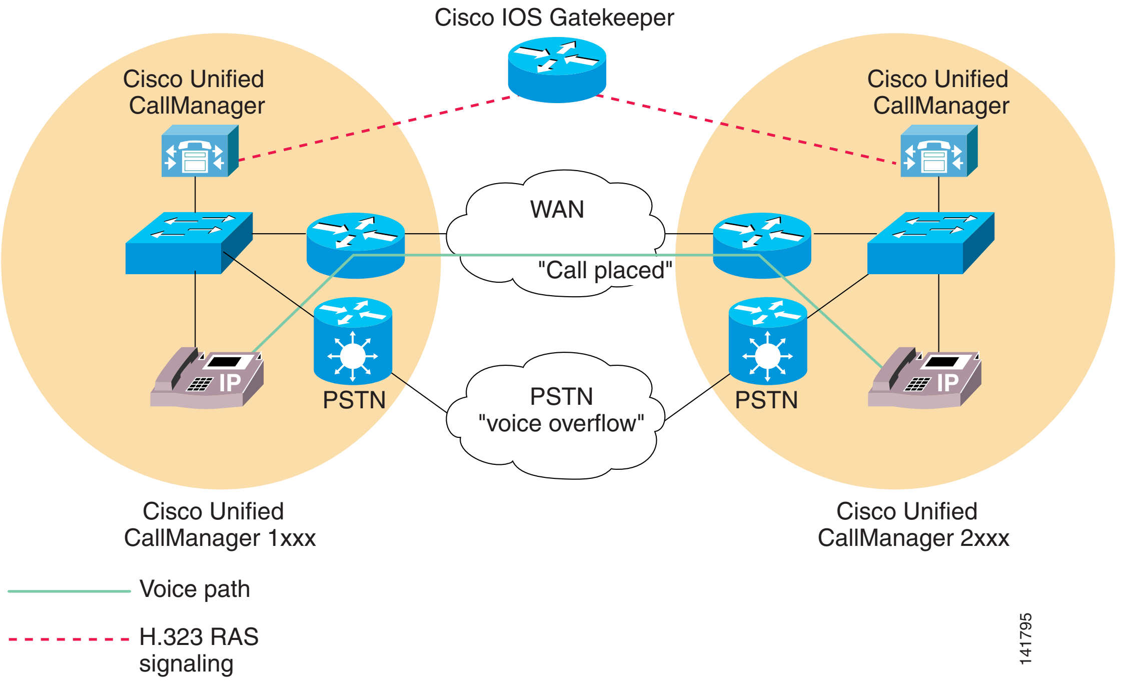
Configuration Steps		Procedures and Related Topics
Step 1	Configure a region for each type of codec that is used in your system.	Locations and Regions, page 8-3 Region Configuration, *Cisco Unified CallManager Administration Guide*.
Step 2	Configure a separate location for each IP WAN link to which you want to apply call admission control. Allocate the maximum available bandwidth for calls across the link to that location. **Note** If you set the bandwidth to *Unlimited*, you allocate unlimited available bandwidth and allow an unlimited number of active calls on the IP WAN link for that location.	Location Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Configure the device pools for your system and choose the appropriate region for each.	Device Pool Configuration, *Cisco Unified CallManager Administration Guide*
Step 4	Configure the phones and other devices and assign each of them to the appropriate device pool and location. **Note** If you set the location to *Hub_None*, you assign that device to an unnamed location with unlimited available bandwidth and allow an unlimited number of active calls to and from that device.	Cisco Unified IP Phones, page 43-1 Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*

Gatekeepers and Trunks

A gatekeeper device, the Cisco Multimedia Conference Manager (MCM), provides call admission control for distributed call-processing systems. In a distributed system, each site contains its own call-processing capability. For example, Figure 8-3 shows two sites, each with its own Cisco Unified CallManager, that an IP WAN link connects. A gatekeeper provides call admission control over the IP WAN link in this example.

In addition to call admission control, gatekeepers can also perform E.164 address resolution to route calls between sites. For example, in Figure 8-3, the extension range for one Cisco Unified CallManager specifies 1XXX and 2XXX for the other. Both register with the gatekeeper for call admission control. Each Cisco Unified CallManager incorporates an appropriate entry in its respective dial plan route pattern configuration that points the other Cisco Unified CallManager extension number range to the gatekeeper. In practice, when user 1001 dials user 2002, Cisco Unified CallManager 1XXX sends 2002 to the gatekeeper for address resolution. If the call satisfies the call admission control criteria, the gatekeeper returns the IP address of Cisco Unified CallManager 2XXX to Cisco Unified CallManager 1XXX. Using the IP address of Cisco Unified CallManager 2XXX, Cisco Unified CallManager 1XXX can then complete the call to directory number 2002.

Figure 8-3 Call Admission Control by Using a Gatekeeper in a Distributed System


Cisco IOS Gatekeeper
Cisco Unified CallManager
Cisco Unified CallManager
WAN
"Call placed"
IP
PSTN
PSTN "voice overflow"
PSTN
IP
Cisco Unified CallManager 1xxx
Cisco Unified CallManager 2xxx
Voice path
H.323 RAS signaling
141795

If the IP WAN is not available in this scenario, the call cannot go through as dialed. To simplify the dial plan and also provide fallback to the PSTN, use 10-digit dialing (or adhere to the national dial plan). For example, under the North American Numbering Plan (NANP), a route pattern of XXXXXXXXXX would direct calls to the gatekeeper for address resolution. If the gatekeeper does not allow the call to go over the WAN, Cisco Unified CallManager can add the prefix 91 to the dialed digits to reroute the call through the PSTN.

Refer to the *Cisco Unified Communications Solution Reference Network Design Guide* for more detailed information about gatekeeper configuration, dial plan considerations when a gatekeeper is used, and gatekeeper interaction with Cisco Unified CallManager.

Sometimes an anonymous H.323 device, a device that is not known to Cisco Unified CallManager, tries to initiate (send or receive) calls with Cisco Unified CallManager. This anonymous device could be a Cisco IOS product (such as a gateway) or any third-party H.323 device.

You can configure H.323 gateways either with gatekeeper control or locally as gateways. If you are configuring with gatekeeper control, or you want to configure an anonymous H.323 device, perform the following steps:

1. Choose **Device > Trunk**.
2. Choose **H.225 Trunk (Gatekeeper Controlled)** from the Trunk Type drop-down list box.
3. When the Trunk Configuration window displays, configure the appropriate fields.

To configure a remote endpoint that Cisco Unified CallManager supports, the administrator performs the following steps:

1. Choose **Device > Trunk**.
2. Choose **Intercluster Trunk (Gatekeeper Controlled)** from the Trunk Type drop-down list box.
3. When the Trunk Configuration window displays, configure the appropriate fields.

To connect two Cisco Unified CallManagers that are in remote clusters, perform the following steps:

1. Choose **Device** > **Trunk**.
2. Choose **Intercluster Trunk (Non-Gatekeeper Controlled)** from the Trunk Type drop-down list box.
3. When the Trunk Configuration window displays, configure the appropriate fields.

See the "Gatekeeper and Trunk Configuration on the Router" section on page 8-8. For information about configuring gatekeeper-controlled intercluster trunks for routing intercluster calls across a remote WAN link, refer to the "Trunk Configuration" section of the *Cisco Unified CallManager Administration Guide* and to the *Cisco Unified Communications Solution Reference Network Design Guide*.

Components of Gatekeeper Call Admission Control

Gatekeeper call admission control provides great flexibility:

- Gatekeepers reduce configuration overhead by eliminating the need to configure a separate H.323 device for each remote Cisco Unified CallManager that is connected to the IP WAN.
- A gatekeeper can determine the IP addresses of devices that are registered with it, or you can enter the IP addresses explicitly.
- The gatekeeper supports the H.323 protocol and uses the H.225 protocol to make calls.
- The gatekeeper can perform basic call routing in addition to call admission control.
- You can connect up to 100 Cisco Unified CallManager clusters to a single gatekeeper.

The following sections describe the components of gatekeeper call admission control:

- Gatekeeper and Trunk Configuration on the Router, page 8-8
- Gatekeeper and Trunk Configuration in Cisco Unified CallManager, page 8-9

Gatekeeper and Trunk Configuration on the Router

Recommended platforms for the gatekeeper include Cisco 2600, 3600, 3700, or 7200 routers with Cisco IOS Release 12.1(3)T or higher. When configuring the gatekeeper function on one of these routers, you define a set of zones for call admission control. The unique name for each zone includes the IP address of each Cisco Unified CallManager that registers with that zone, the zone prefix (directory number range), and the bandwidth that is allocated for that zone.

Cisco Unified CallManager registers with a gatekeeper by using its IP address. You can specify the IP address in one of the following ways:

- Use the **gw-type-prefix** command on the gatekeeper to specify each Cisco Unified CallManager IP address explicitly.
- In the Technology Prefix field under **Device** > **Trunk** in Cisco Unified CallManager Administration, enter **1#*** and enter the command **gw-type-prefix 1#* default-technology** on the gatekeeper. When a Cisco Unified CallManager registers with the gatekeeper, it sends its IP address and the specified technology prefix to the gatekeeper. The gatekeeper then registers this Cisco Unified CallManager as a valid gatekeeper-controlled VoIP device.

You associate the Cisco Unified CallManager IP address with a particular zone by performing the following steps:

- Use the **zone local** command on the gatekeeper to define local zones. Enter the zone name in the Zone field.

- In the Zone field under **Device** > **Trunk** in Cisco Unified CallManager Administration, enter the zone name. When a Cisco Unified CallManager registers with the gatekeeper, it sends its IP address and the specified zone name to the gatekeeper. The gatekeeper then registers each Cisco Unified CallManager and associates it with the appropriate zone.

To specify the directory number range for a particular Cisco Unified CallManager, you use the **zone prefix** command to configure the range on the gatekeeper. For example, the following command specifies that the DN for zone LHR ranges from 3000 to 3999.

```
zone prefix LHR 3...
```

The maximum number of active calls that are allowed per zone depends on the codec that is used for each call and the bandwidth that is allocated for the zone. With Cisco Unified CallManager, G.711 calls request 128 kbps, and G.723 and G.729 calls request 20 kbps. Use regions in Cisco Unified CallManager to specify the codec type and use the **bandwidth total zone** command on the gatekeeper to specify the available bandwidth. For example, the following command allocates 512 kbps to the LHR zone.

```
bandwidth total zone LHR 512
```

With an allocation of 512 kbps, the LHR zone in this example could support up to four G.711 calls at the same time.

For more information on programming the gatekeeper, refer to the Configuring H.323 Gatekeepers and Proxies section of the *Cisco IOS H.323 Configuration Guide*.

Gatekeeper and Trunk Configuration in Cisco Unified CallManager

You can configure gatekeepers and trunks in Cisco Unified CallManager administration to function in either of the following ways:

Non-Gatekeeper-Controlled Trunks

In this case, you explicitly configure a separate intercluster trunk for each remote device cluster that the local Cisco Unified CallManager can call over the IP WAN. You also configure the necessary route patterns and route groups to route calls to and from the various intercluster trunks. The intercluster trunks statically specify the IP addresses of the remote devices. To choose this method, use **Device** > **Trunk** and select Inter-Cluster Trunk (Non-Gatekeeper Controlled) in Cisco Unified CallManager Administration.

Note For a local non-gatekeeper-controlled intercluster trunk, you must specify the IP addresses of all remote Cisco Unified CallManager nodes that belong to the device pool of the remote non-gatekeeper-controlled intercluster trunk.

Gatekeeper-Controlled Trunks

In this case, a single intercluster trunk suffices for communicating with all remote clusters. Similarly, you need a single H.225 trunk to communicate with any H.323 gatekeeper-controlled endpoints. You also configure route patterns or route groups to route the calls to and from the gatekeeper. In this configuration, the gatekeeper dynamically determines the appropriate IP address for the destination of each call to a remote device, and the local Cisco Unified CallManager uses that IP address to complete the call.

This configuration works well in large as well as smaller systems. For large systems where many clusters exist, this configuration helps to avoid configuring individual intercluster trunks between each cluster. To choose this method, use **Device** > **Trunk** and select Inter-Cluster Trunk (Gatekeeper Controlled) in Cisco Unified CallManager Administration.

If you configure gatekeeper-controlled trunks, Cisco Unified CallManager automatically creates a virtual trunk device. The IP address of this device changes dynamically to reflect the IP address of the remote device as determined by the gatekeeper. Use trunks when configuring the route patterns or route groups that route calls to and from a gatekeeper.

Gatekeeper and Trunk Configuration Checklist

Table 8-2 lists the general steps for configuring call admission control that is based on gatekeepers and trunks.

Table 8-2 Gatekeeper and Trunk Configuration Checklist

Configuration Steps		Procedures and related topics
Step 1	On the gatekeeper device, configure the appropriate zones and bandwidth allocations for the various Cisco Unified CallManagers that will route calls to it.	Configuring H.323 Gatekeepers and Proxies, *Cisco IOS H.323 Configuration Guide*
Step 2	Configure gatekeeper settings in Cisco Unified CallManager Administration. Repeat this step for each Cisco Unified CallManager that will register with the gatekeeper. Make sure Host Name or IP Address is set the same way on each Cisco Unified CallManager.	Gatekeeper Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Configure the appropriate intercluster trunks or H.225 trunks to specify gatekeeper information (if gatekeeper-controlled).	Trunk Configuration, *Cisco Unified CallManager Administration Guide*
Step 4	Configure a route pattern to route calls to each gatekeeper-controlled trunk.	Understanding Route Plans, page 17-1 Route Pattern Configuration, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topics

- Location Configuration, *Cisco Unified CallManager Administration Guide*
- Region Configuration, *Cisco Unified CallManager Administration Guide*
- Route Pattern Configuration, *Cisco Unified CallManager Administration Guide*
- Gatekeeper Configuration, *Cisco Unified CallManager Administration Guide*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide*
- Resource Reservation Protocol, page 9-1
- Cisco Unified IP Phones, page 43-1
- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*

- Understanding Video Telephony, page 44-1
- Trunk Configuration, *Cisco Unified CallManager Administration Guide*
- Multilevel Precedence and Preemption, *Cisco Unified CallManager Features and Services Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design for Cisco Unified CallManager*
- Cisco Multimedia Conference Manager (Command Reference) IOS documentation

Resource Reservation Protocol

Resource Reservation Protocol (RSVP) specifies a resource-reservation, transport-level protocol for reserving resources in IP networks. RSVP provides an additional method to achieve call admission control (CAC) besides location-based CAC. The following factors call for RSVP support as an alternative call admission control (CAC) mechanism in Cisco Unified CallManager:

- Many customers request a full-mesh network topology for their video conferencing and video telephony environment to match their existing topology. If Cisco Unified CallManager does not support an RSVP-based CAC mechanism, these customers must move to a hub-and-spoke topology.
- The growing size of a Cisco Unified CallManager cluster increases the need for an intracluster CAC solution.
- Cisco Unified CallManager video support with video-enabled endpoints requires an alternative CAC mechanism.
- The Quality of Service (QoS) baseline requires all VoIP and videoconferencing devices to provide admission control using RSVP.

For a discussion of call admission control (CAC), see Chapter 8, “Call Admission Control.”

This section provides an overview of RSVP, describes RSVP configuration within Cisco Unified CallManager, discusses migration to RSVP, shows example RSVP configurations, and provides troubleshooting information. See the following topics:

- RSVP Overview, page 9-1
- RSVP Agent and Quality of Service, page 9-5
- RSVP Configuration, page 9-6
- Migrating to RSVP, page 9-13
- Example RSVP Interactions, page 9-15
- Troubleshooting RSVP, page 9-21
- Where to Find More Information, page 9-23

RSVP Overview

RSVP includes the following features:

- RSVP reservations get made for a particular session. A session comprises a flow that has a particular destination address, destination port, and a protocol identifier (TCP or UDP). RSVP reservations treat each session as one independent unit.

- RSVP messages travel along the same path as the media flow path.
- Because RSVP is unidirectional, flows get reserved in only one direction.
- Because RSVP is receiver-oriented, the receiver of the stream requests the reservation.
- RSVP supports both unicast and multicast environments.
- RSVP messages flow transparently through non-RSVP routers and switches.

Advantages of RSVP

The following factors make RSVP a more desirable solution than location-based call admission control (CAC) for providing quality of service (QoS):

- RSVP can handle complex topologies. Location-based CAC only supports hub-and-spoke network topologies. Location-based CAC does not handle complex topologies, such as the following
  - Redundant links (A = B)
  - More than three sites in a series (A — B — C — D)
  - Multilevel hierarchies (hubs, regions, and subregions)
  - Meshes
- RSVP exhibits network awareness, whereas location-based CAC cannot handle dynamic changes to bandwidth.
- IP videoconferencing not only requires significant bandwidth but also requires specialized service from the network with respect to latency and packet loss. RSVP enables network to accommodate such traffic without unduly degrading the performance of other applications in the network
- RSVP supports Multilevel Precedence and Preemption (MLPP) inherently.

RSVP Capabilities

The following capabilities get built on top of RSVP:

- RSVP supports all signaling protocols, including SIP, SCCP, MGCP, and H.323.
- RSVP works by enforcing a location-pair-based RSVP policy. You can enable and disable RSVP based on location pairs. This practice allows for migration.
- The setting of a systemwide service parameter determines RSVP policy for the system. Therefore, you can enable or disable RSVP throughout the system. Location-pair-based policies, however, override the systemwide policy.
- RSVP provides the following RSVP policy levels:
  - No reservation (Continue using location-based CAC.)
  - Mandatory
  - Optional (video desired)
  - Mandatory (video desired)
- RSVP contains a Retry reservation capability. This capability allows a call to gain or regain premium Quality of Service (QoS) even if the resources (bandwidth) are not currently available.

- The RSVP Retry Timer controls the frequency of retry. The Mandatory RSVP Mid-call Retry Counter and Mandatory RSVP mid call error handle option service parameters control the number of attempts to restore premium service by reserving the necessary resources if the initial RSVP policy specifies Mandatory.
- RSVP integrates with Differentiated Services (DiffServ) QoS. The outcome of an RSVP reservation updates the Differentiated Services Code Point (DSCP) value.
- RSVP has a midcall failure policy. This capability allows a user to determine what happens to the call if the call loses the bandwidth reservation in mid call. The following options exist:
  - The call fails after N reservation retries.
  - The call becomes a best-effort call.
- RSVP supports bandwidth reservation for both audio and video streams. RSVP provides application ID support.
- RSVP supports Multilevel Precedence and Preemption (MLPP).
- RSVP retains the reservation when a party gets put on hold. The reserved resource(s) can potentially get reused when the call resumes.
- Shared-line devices that are located in the same location/region share the same reservation for incoming calls.
- RSVP works with all Cisco Unified CallManager supplementary services and features to ensure that bandwidth reservation is correct after the service or feature is invoked. Examples of supported features include Call Transfer, Conference, and Call Forwarding.
- RSVP supports Music on Hold (MOH) and annunciator features.

RSVP-Based MLPP

When RSVP is configured, MLPP functions as follows:

- Cisco Unified CallManager passes the precedence level of the MLPP call to the RSVP Agent by means of SCCP Quality of Service (QoS) messages.
- Agents add priority information to RSVP requests.
- IOS routers can use this priority information to admit calls.
- If preemption occurs at the IOS router, the RSVP Agent notifies Cisco Unified CallManager about the reservation failure due to preemption.
- Cisco Unified CallManager notifies the preempted calling party and called party of the preemption. Cisco Unified CallManager uses the existing MLPP functionality, which resembles the location-based call admission control (CAC) MLPP preemption mechanism.
- Preempted calls can either fail or continue with decreased QoS. Preempted calls receive the same treatment as midcall reservation failure.

Additional Features

Cisco Unified CallManager supports the following interactions:

- RSVP Agent supports Differentiated Services Control Point (DSCP) remarking. This capability mitigates the trust issues with desktop applications, such as Communicator and VTA.

- RSVP supports audio, video, and data pass-through. Video data pass-through allows video and data packets to flow through RSVP Agent and Media Termination Point devices. Video data pass-through also allows audio transcoding to work with video calls. Audio pass-through allows encrypted calls to flow through MTPs.

Pass-Through Conditions

The following conditions apply to both audio and video/data pass-through:

- All intermediate MTP devices support pass-through.
- No “MTP required” check box is checked for either endpoint.

The following additional audio pass-through condition applies:

- A matching audio cap exists between two endpoints after region filtering.

The following additional video pass-through condition applies:

- All intermediate MTP devices support multimedia. That is, MTP devices support multiple channels per call.

RSVP Caveats

RSVP presents the following support limitations:

- RSVP does not support intercluster RSVP Agents.That is, RSVP does not support reservations between two RSVP Agents that are located in different clusters.

  Consider the following scenario:

  endpoint A — agentA — agentICT1 — ICT1 — ICT2 — agentICT2 — agentB — endpoint B

  where A specifies an endpoint in cluster 1, B specifies an endpoint in cluster 2, ICT1 and ICT2 specify the intercluster trunks within clusters 1 and 2, and the RSVP Agents associate with the respective devices.

  In this scenario, Cisco Unified CallManager 1 controls the reservation between agentA and agentICT1, and Cisco Unified CallManager 2 controls the reservation between agentB and agentICT2.

  As an alternative, IP-IP gateways can be used. See the “Gatekeepers and Trunks” section on page 8-6 for more information.
- Cisco Unified CallManager does not support RSVP interaction with endpoints that support RSVP natively.
- Cisco Unified CallManager does not support device mobility. Because a device’s Media Resource Group List (MRGL) is configured statically, the MRGL does not get updated automatically when the device moves.

Note RSVP does not conflict with Automated Alternate Routing (AAR), which continues to function if AAR is configured. See the “Automated Alternate Routing” section on page 17-1 for details.

RSVP Agent and Quality of Service

Cisco Unified CallManager uses an RSVP Agent, which is an IOS-based RSVP proxy with an SCCP interface to support RSVP. Cisco Unified CallManager communicates with the RSVP Agent through a set of SCCP messages. The RSVP Agent registers with Cisco Unified CallManager as either a media termination point or a transcoder device.

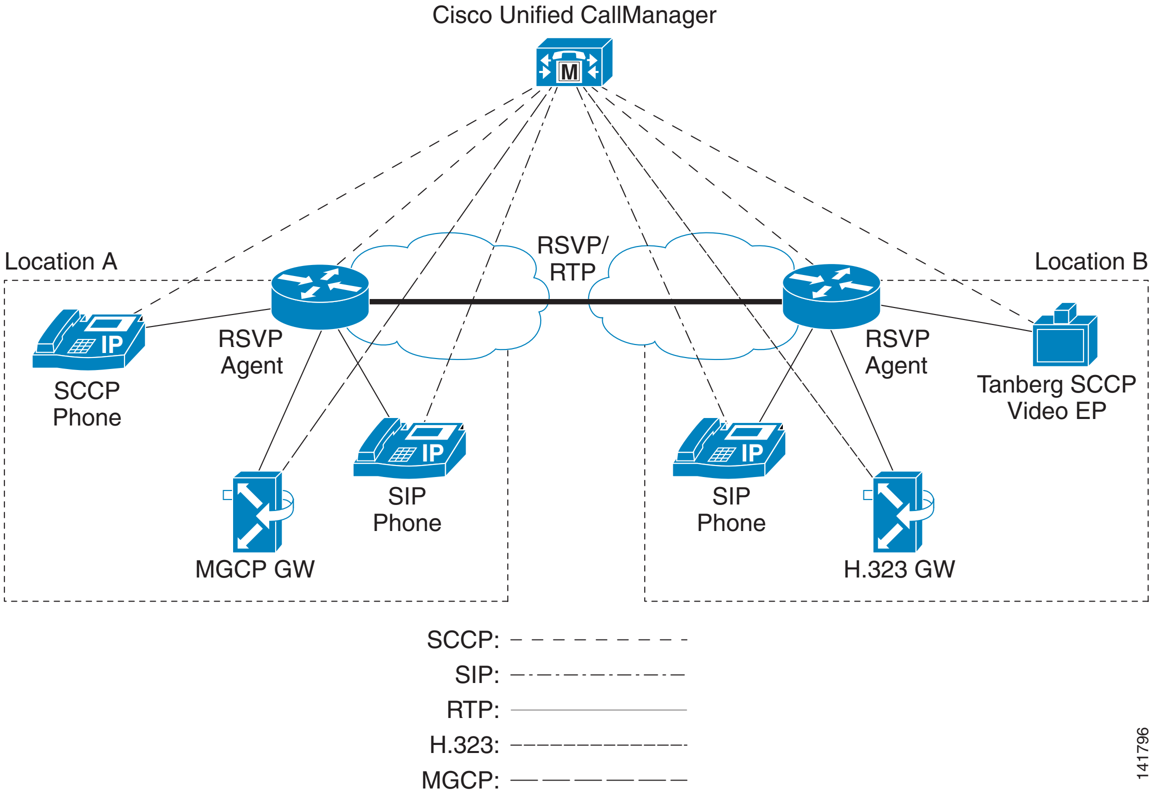
Each endpoint requires an RSVP Agent. The agent pair (one agent for endpoint A, another agent for endpoint B) signals RSVP on behalf of the endpoints that Cisco Unified CallManager controls.

Why an Agent?

An agent provides the means to support RSVP for all endpoints whether the endpoint supports RSVP natively or not. An agent provides a point of trust and eases migration to RSVP.

Figure 9-1 shows an example of a Cisco Unified CallManager network with RSVP configured through an RSVP Agent.

Figure 9-1 Cisco Unified CallManager Network Configured with RSVP Agent



RSVP Agent Allocation

Cisco Unified CallManager allocates the RSVP Agent resource in the same manner that it allocates media termination point and transcoder resources. You configure a Media Resource Group List (MRGL) that includes the RSVP Agent and assign the MRGL to the device or the device pool that associates with the device. RSVP reservation fails if the same RSVP Agent is assigned to both endpoints that are making a call.

RSVP Agent Interaction with Location-Based CAC

Cisco recommends that you do not activate both location-based Call Admission Control (CAC) and RSVP at the same time, except during the migration period from location-based CAC to RSVP.

If location bandwidth is not set to unlimited (infinite bandwidth) in the location, Cisco Unified CallManager performs location-based CAC before performing RSVP. If location-based CAC fails, the call fails, and Cisco Unified CallManager does not invoke RSVP.

If location bandwidth is set to unlimited (infinite bandwidth) in the location, Cisco Unified CallManager invokes RSVP based on RSVP policy for the location pair that is associated with the calling and the called parties.

RSVP Configuration

RSVP configuration comprises configuration of various service parameters and other components. The sections that follow describe the various service parameters and other configuration that is needed to configure RSVP. See the following topics:

- Clusterwide Default RSVP Policy, page 9-7
- Location-Pair RSVP Policy, page 9-7
- RSVP Retry, page 9-8
- Mid-call RSVP Error Handling, page 9-8
- MLPP-to-RSVP Priority Mapping, page 9-9
- TSpec, page 9-9
- DSCP, page 9-11
- Application ID, page 9-11
- RSVP for Media Devices, page 9-11
- Enabling RSVP for a Call, page 9-11
- Special Configuration With RSVP, page 9-12
- RSVP Configuration Checklist, page 9-12

Clusterwide Default RSVP Policy

To configure the clusterwide RSVP policy, configure the following clusterwide (System - RSVP) service parameter for the Cisco CallManager service:

1. In Cisco Unified CallManager Administration, choose the **System > Service Parameters** menu option.
2. In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.
3. In the Clusterwide Parameters (System — RSVP) section, configure the Default interlocation RSVP Policy service parameter.

You can set this service parameter to the following values:

- No Reservation—No RSVP reservations get made between any two locations.
- Optional (Video Desired)—A call can proceed as a best-effort, audio-only call if failure to obtain reservations for both audio and video streams occurs. RSVP Agent continues to attempt RSVP reservation for audio and informs Cisco Unified CallManager if reservation succeeds.
- Mandatory—Cisco Unified CallManager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream as well.
- Mandatory (Video Desired)—A video call can proceed as an audio-only call if a reservation for the audio stream succeeds but a reservation for the video stream does not succeed.

See the "Service Parameters Configuration" section of the *Cisco Unified CallManager Administration Guide* for additional information about service parameters.

Location-Pair RSVP Policy

Use the Location Configuration window to configure the RSVP policy for a given location pair. The RSVP policy that is configured for a location pair overrides the default interlocation RSVP policy that you configure in the Service Parameter Configuration window.

To configure the RSVP policy for a pair of locations, configure the RSVP Setting field for the location pair:

1. In Cisco Unified CallManager Administration, choose the **System > Location** menu option.
2. Find one location of the location pair and select this location.
3. To modify the RSVP policy between the selected location and another location, select the other location in the location pair.
4. In the RSVP Setting drop-down list box, choose an RSVP policy for this location pair.

You can set this field to the following values:

- Use System Default—The RSVP policy for the location pair matches the clusterwide RSVP policy. See the "Clusterwide Default RSVP Policy" section on page 9-7 for details.
- No Reservation—No RSVP reservations get made between any two locations.
- Optional (Video Desired)—A call can proceed as a best-effort, audio-only call if failure to obtain reservations for both audio and video streams occurs. RSVP Agent continues to attempt RSVP reservation for audio and informs Cisco Unified CallManager if reservation succeeds.
- Mandatory—Cisco Unified CallManager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream as well.

- Mandatory (Video Desired)—A video call can proceed as an audio-only call if a reservation for the audio stream succeeds but the reservation for the video stream does not succeed.

RSVP Retry

Use the following clusterwide (System - RSVP) service parameters to configure the frequency and number of RSVP retries:

- RSVP Retry Timer
- Mandatory RSVP Mid-call Retry Counter

To locate and configure these service parameters, follow these steps:

1. In Cisco Unified CallManager Administration, choose the **System > Service Parameters** menu option.
2. In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.
3. In the Clusterwide Parameters (System — RSVP) section, configure the specified service parameters.

You can set these service parameters to the following values:

- RSVP Retry Timer—Specify the RSVP retry timer value in seconds. If you set this parameter to 0, you disable RSVP retry on the system.
- Mandatory RSVP Mid-call Retry Counter—Specify the midcall RSVP retry counter when the RSVP policy specifies Mandatory and midcall error handling option is set to “call fails following retry counter exceeds.” The default value specifies 1 time. If you set the service parameter to -1, retry continues indefinitely until either the reservation succeeds or the call gets torn down.

See the “Service Parameters Configuration” section of the *Cisco Unified CallManager Administration Guide* for additional information about service parameters.

Mid-call RSVP Error Handling

Use the following clusterwide (System - RSVP) service parameter to configure mid-call RSVP error handling:

- Mandatory RSVP mid call error handle option

To locate and configure this service parameter, follow these steps:

1. In Cisco Unified CallManager Administration, choose the **System > Service Parameters** menu option.
2. In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.
3. In the Clusterwide Parameters (System — RSVP) section, configure the specified service parameter.

You can set the Mandatory RSVP mid call error handle option service parameter to the following values:

- Call becomes best effort—If RSVP fails during a call, the call becomes a best-effort call. If retry is enabled, RSVP retry attempts begin simultaneously.
- Call fails following retry counter exceeded—If RSVP fails during a call, the call fails after N retries of RSVP, where the Mandatory RSVP Mid-call Retry Counter service parameter specifies N.

See the "Service Parameters Configuration" section of the *Cisco Unified CallManager Administration Guide* for additional information about service parameters.

MLPP-to-RSVP Priority Mapping

Use the following clusterwide (System - RSVP) service parameters to configure the mapping from a caller's MLPP precedence level to RSVP priority:

- MLPP EXECUTIVE OVERRIDE To RSVP Priority Mapping
- MLPP FLASH OVERRIDE To RSVP Priority Mapping
- MLPP FLASH To RSVP Priority Mapping
- MLPP IMMEDIATE To RSVP Priority Mapping
- MLPP PL PRIORITY To RSVP Priority Mapping
- MLPP PL ROUTINE To RSVP Priority Mapping

To locate and configure these service parameters, follow these steps:

1. In Cisco Unified CallManager Administration, choose the **System > Service Parameters** menu option.
2. In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.
3. In the Clusterwide Parameters (System — RSVP) section, configure the specified service parameters.

These service parameters function as follows:

- Cisco Unified CallManager maps the caller's precedence level to RSVP priority when initiating an RSVP reservation based on the following configuration: the higher the service parameter value, the higher the priority.
- The IOS router preempts the call based on RSVP priority.
- The RSVP Agent must notify Cisco Unified CallManager about the reason for an RSVP reservation failure, including the cause for preemption.
- Cisco Unified CallManager uses the existing MLPP mechanism to notify the preempted calling and called parties about the preemption.

See the "Service Parameters Configuration" section of the *Cisco Unified CallManager Administration Guide* for additional information about service parameters.

TSpec

The TSpec object describes the traffic that the sender generates. The TSpec gets transported through the network to all intermediary routers and to the destination endpoint. The intermediate routers do not change this object and the object gets delivered unchanged to the ultimate receiver(s).

The TSpec object comprises the following elements:

- averageBitRate (kbps)
- burstSize (bytes)
- peakRate (kbps)

Audio TSpec

For audio flows, the TSpec calculations specify the following measurements:

- burstSize (bytes)—This value gets calculated as the size of the packet times the number of packets in a burst. For audio flows, the burst usually specifies 1 to 2.
- peakRate (bytes)—The peakRate, in bytes, refers to the maximum bytes/second that the endpoint transmits at any given time. If the burst is small, as is the case in audio streams, the peakRate can be calculated as 1.1 (or 1.2) times the tokenRate.

To avoid adjusting the bandwidth reservation upward when the call gets answered,
Cisco Unified CallManager reserves the maximum bandwidth for each region codec at call setup time. Cisco Unified CallManager then modifies or adjusts the bandwidth based on the media capability of the connected parties when the call gets answered.

Example Audio TSpec Calculations

See the following examples of bandwidth calculations for different region codecs for call setup.

G.711: 8 sample/frame; for 10-ms packet: 80 + 40 (header) = 120 * 100 (packets/sec) = 12000 * 8 = **96 kbps**; (packet_size_in_ms*8+40)*8000/packet_size_in_ms

G.729: 10 ms/frame; 8 kbps; Default is 20 ms; 0 and 10 are possible. For 10-ms packet: 10 + 40 = 50 * 100 = 5000 * 8 = **40 kbps**

kbps: (packet_size_in_ms+40)*8000/packet_size_in_ms

The TSpec of the G.711 codec specifies the following calculations:

Tspec.mAverageBitRate = bwPlusHeader = 96 kbps;

Tspec.mPeakRate = Tspec.mAverageBitRate * (1.2) = 115;

Tspec.mBurstSize = PacketSize * 2 = 120 * 2 = 240;

Video TSpec

For video streams, the packet length does not depend on codecs. Individual implementations provide the basis for packet length. Also, the packet sizes do not remain uniform across all packets. Estimating the number of packets per second therefore proves difficult.

Assume that the maximum packet size for a video stream specifies 1000 bytes.

The RSVP Video Tspec Burst Size Factor service parameter in the Clusterwide Parameters (System - RSVP) section of the service parameters for the Cisco CallManager service allows you to configure the video stream burst size. The default value for this service parameter specifies 5.

The following elements comprise the video Tspec:

- burstSize (bytes)—Burst size factor (5) * max packet size (1000)
- peakRate (bytes)—This element refers to the maximum bytes/second that the endpoint transmits at any given time. If the burst is small, as is the case with audio streams, you can calculate the peakRate as 1.1 (or 1.2) times the tokenRate.

Cisco Unified CallManager attempts to use the bandwidth for the entire video call to reserve bandwidth for the video stream first: 384 kb + overhead.

Example: 384 + 27 = 410 kbps

If insufficient bandwidth exists for the entire video call, Cisco Unified CallManager next attempts to reserve the following amount of bandwidth: (video call bandwidth - audio stream codec) + overhead).

Example: (384 - 64) + 22 = 342 kbps

The Tspec for the 384 kb codec specifies the following calculations:

Tpsec.mAverageBitRate = bwPlusHeader = 410 kbps;

Tspec.mPeakRate = Tspec.mAverageBitRate = 410;

Tspec.mBurstSize = 1000 * 5 = 5000;

DSCP

If RSVP reservation fails, Cisco Unified CallManager instructs the RSVP Agent or endpoint devices (in case failure to allocate an RSVP Agent occurs) to change media Differentiated Services Control Point (DSCP) marking to best effort. Otherwise, an excess of EF-marked media packets can degrade quality of service (QoS) even for flows that have a reservation.

Cisco Unified CallManager uses the clusterwide (System - QoS) DSCP for Audio Calls When RSVP Fails service parameter or the DSCP for Video Calls When RSVP Fails service parameter to determine the DSCP values for this instruction when RSVP fails for the call.

Application ID

An application ID specifies an RSVP object that can be inserted in a policy element in an RSVP message. RFC 2872 describes this object. This policy object serves to identify the application and associates the application with the RSVP reservation request, thus allowing routers along the path to make appropriate decisions based on the application information.

The following clusterwide (System - RSVP) system parameters allow configuration of application IDs:

- RSVP Audio Application ID
- RSVP Video Application ID

RSVP for Media Devices

Because conference bridges, music on hold servers, and annunciators do not specify Media Resource Group List (MRGL) configuration, you make RSVP resources available for these devices by associating these devices with a device pool that has an associated RSVP Agent. The MRGL that is associated with the device pool gets used to allocate RSVP resources for these types of media devices.

Enabling RSVP for a Call

To enable RSVP for a call, follow these steps:

1. Assign the calling device and the called device to different locations.
2. Either configure default interlocation policy to any setting other than “No Reservation” or use the Location Configuration window to configure the RSVP setting for the two locations to anything other than “No Reservation.”
3. Assign a Media Resource Group List that includes an RSVP Agent resource to both endpoint devices. Use either the configuration window for the devices or the Device Pool Configuration window.

Special Configuration With RSVP

In an RSVP session, special configuration applies if all the following conditions exist:

- One endpoint device, such as Cisco IP Interactive Voice Response (IP IVR), was configured to support only the G.711 codec.
- RSVP was configured for the call.
- The interregion codec specifies G.729 between the calling RSVP Agent and the called RSVP Agent.

When the call is made, to achieve successful allocation and reservation of RSVP Agent resources and bandwidth, the administrator must configure the media termination point (MTP)/RSVP Agent with the G.729 codec in addition to the pass-through codec. This configuration allows insertion of a transcoder between the RSVP Agent of the called side and the called device at the time of media connection. When codecs match, codec pass-through takes place; if codecs do not match, the call cannot continue without a transcoder.

If configuration of the G.729 codec in the agent does not take place, the call will fail because Cisco Unified CallManager will not invoke a transcoder that is needed for the RSVP call.

The situation arises if either of the following conditions apply: the interregion codec gets used between calling and called agents or between two endpoints that specify G.729. Two options exist to enable successful routing of this call:

- Use RSVP Agent for IVR as a transcoder. In this case, the interregion codec between the transcoder/RSVP Agent and IVR needs to specify the G.711 codec.
- Use software MTP as RSVP Agents and insert a transcoder between IVR and the RSVP Agent for IVR. In this case, ensure the software MTP is configured with the G.729 codec in addition to the pass-through codec.

Keep in mind that the RSVP Agent that has transcoding capability cannot perform G.729-to-G.729 transcoding. If you use a transcoder as an RSVP Agent, you either must use the pass-through codec or configure the transcoder, so one of the codecs that is used on both sides of the transcoder specifies G.711.

RSVP Configuration Checklist

Table 9-1 lists the general steps for configuring call admission control by using RSVP.

Table 9-1 RSVP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Configure the clusterwide default RSVP policy.	RSVP Configuration, page 9-6 Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
Step 2	Configure the RSVP policy for any location pair that requires a different RSVP policy from the clusterwide default RSVP policy.	Location Configuration, *Cisco Unified CallManager Administration Guide*

Table 9-1 RSVP Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 3	Configure other RSVP-related service parameters: • RSVP Retry • Mid-call RSVP Error Handling • MLPP-to-RSVP Priority Mapping • TSpec • DSCP • Application ID	RSVP Configuration, page 9-6 Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
Step 4	Configure RSVP Agents for media devices.	RSVP for Media Devices, page 9-11 Device Pool Configuration, *Cisco Unified CallManager Administration Guide* Media Resource Group List Configuration, *Cisco Unified CallManager Administration Guide*
Step 5	Enable RSVP for a call.	Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide* Media Resource Group List Configuration, *Cisco Unified CallManager Administration Guide*

Migrating to RSVP

Migration from location-based call admission control (CAC) to RSVP requires that you take some special circumstances into consideration. During the RSVP deployment time period, devices in some locations will probably have RSVP Agent configured while others do not have RSVP Agent configured.

When a call takes place from a location that has RSVP Agent to another location that does not have RSVP Agent, Cisco Unified CallManager will manage the quality of service (QoS) of the call by using both location-based CAC and RSVP. The first part of the call, from the location that has RSVP Agent to the hub/central site that has RSVP, uses the RSVP mechanism. The second part of the call, from the hub/central site to the location that does not have RSVP, gets managed through location-based CAC. If either mechanism fails to allocate bandwidth, the call fails.

Example

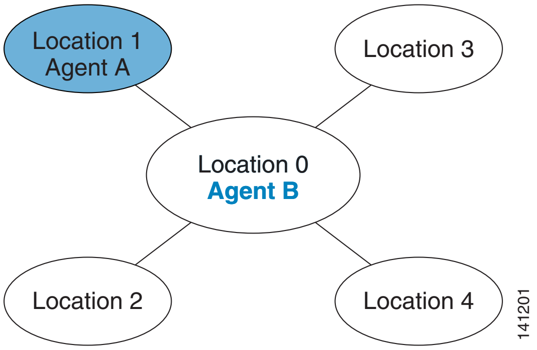
The following steps show how to migrate the first location and hub to RSVP.

1. Install RSVP Agent A at Location 1.
2. Install RSVP Agent B at Location 0 (hub).
3. Add Agent A to the Media Resource Group List of all endpoints at Location 1.
4. Add Agent B to the Media Resource Group List of all endpoints not at Location 1, including devices at the hub and at all other locations.

5. Configure RSVP policy from Location 1 to all other locations to be Mandatory (or some other policy, if desired).
6. Change the location CAC bandwidth limit for Location 1 to unlimited.

Figure 9-2 shows a location configuration to which the migration process applies.

Figure 9-2 Migrating the First Spoke of a Location Configuration



After you perform the preceding configuration steps, the following bandwidth applies to the locations:

Location	Bandwidth
0	Unlimited
1	Unlimited
2	1500
3	3000
4	3000

After you perform the preceding configuration steps, the following RSVP policies apply:

Location Pair		RSVP Policy
1	1	None
1	Not 1	Mandatory
Not 1	Not 1	None

After you take the preceding configuration steps, the following call admission control (CAC) takes place:

- Calls within locations 0, 2, 3, and 4 use the same CAC as before.
- Calls within location 1 are not subject to CAC.
- Calls between location 0 and location 1 use RSVP CAC.
- Calls between location 1 and locations 2, 3, or 4 have RSVP on the 0-to-1 link and location-based CAC on the 0-to- 2, 0-to-3, or 0-to-4 link. If either mechanism fails, the call fails.

Example RSVP Interactions

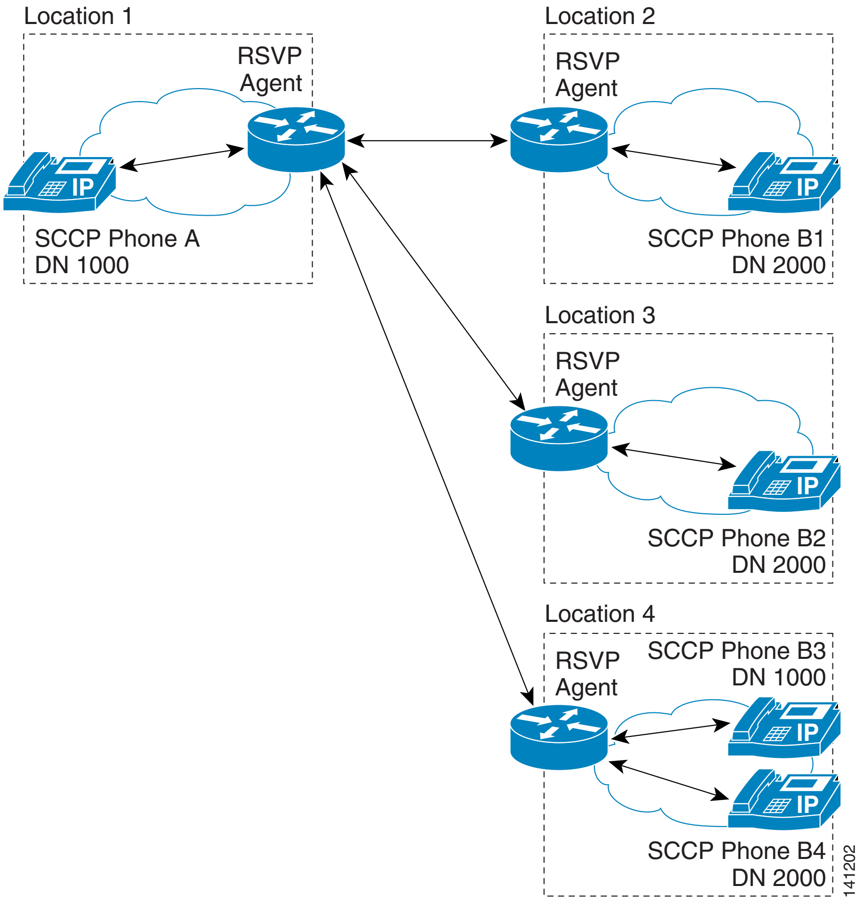
The following sections provide examples of RSVP interaction with various Cisco Unified CallManager features and services. See the following topics:

- RSVP and Shared-Line Calls, page 9-15
- RSVP and Music On Hold, page 9-16
- RSVP and Call Transfer, page 9-18
- RSVP and MLPP, page 9-20

RSVP and Shared-Line Calls

Figure 9-3 shows the RSVP interaction during the alerting phase of a shared-line call.

Figure 9-3 RSVP During a Shared--Line Call (Alerting Phase)



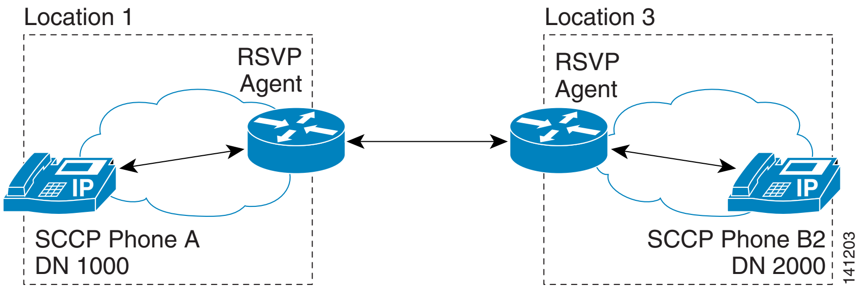
The example shows the following configuration during the alerting phase of the shared-line call:

- Phones B1 (in location 2), B2 (in location 3), and B3 and B4 (both in location 4) share the DN 2000.
- The RSVP Agent in location 1 has a single allocated port. The port has multiple destinations, one to each RSVP Agent in the other locations (2, 3, and 4).
- RSVP Agent in location 4 has one allocated port. Phones B3 and B4 share this port.

Phones B3 and B4, which share the DN 2000, use a single RSVP Agent.

Figure 9-4 shows the RSVP interaction after a shared-line call gets answered.

Figure 9-4 RSVP During a Shared-Line Call (Call Answered Phase)

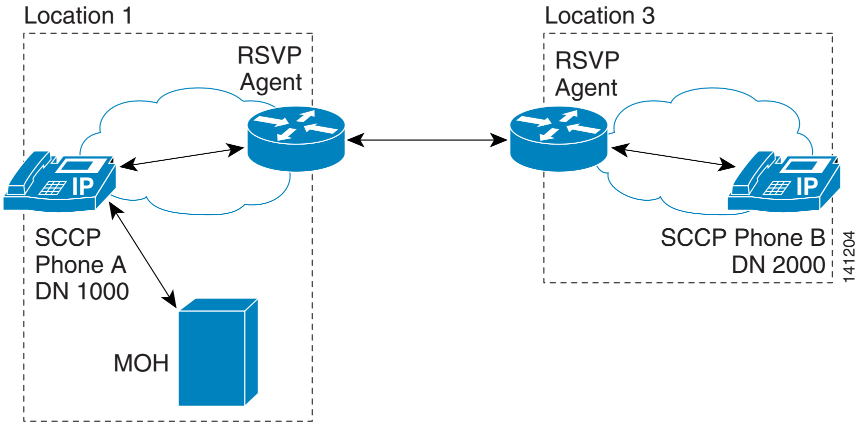


After phone B2 (in location 3) answers the shared-line call, the RSVP reservation between location 1 and location 3, as well as the reservation between location 1 and location 4, get torn down.

RSVP and Music On Hold

Figure 9-5 shows a call that invokes Music On Hold. Phones A and B are in a call when phone B puts phone A on hold. In Figure 9-5, the MOH server resides in the same location as phone A.

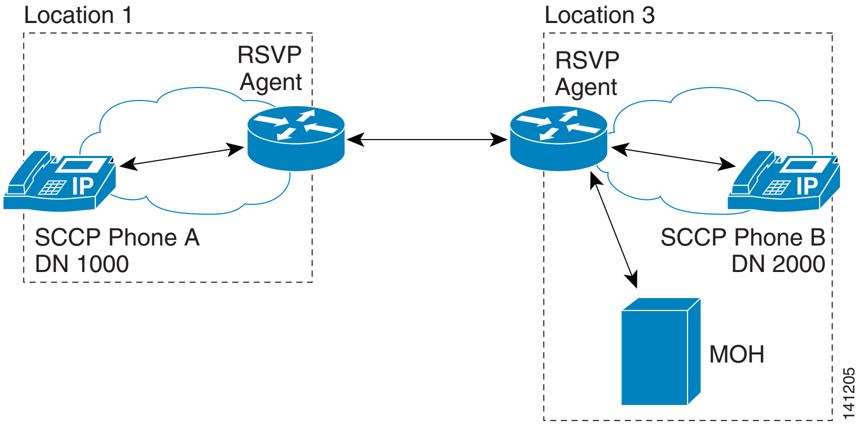
Figure 9-5 Phone B Puts Phone A on Hold, MOH Server in Same Location as Phone A



RSVP preserves the reservation between phone A and phone B while phone A is on hold and receiving Music On Hold. After the call between phone A and phone B resumes, the reserved resource gets reused. Because phone A and the MOH server that provides its music on hold are in the same location, no need exists for RSVP reservation between phone A and the MOH server.

Figure 9-6 shows a call that invokes Music On Hold. Phones A and B are in a call when phone B puts phone A on hold. In the illustration, the MOH server resides in the same location as phone B.

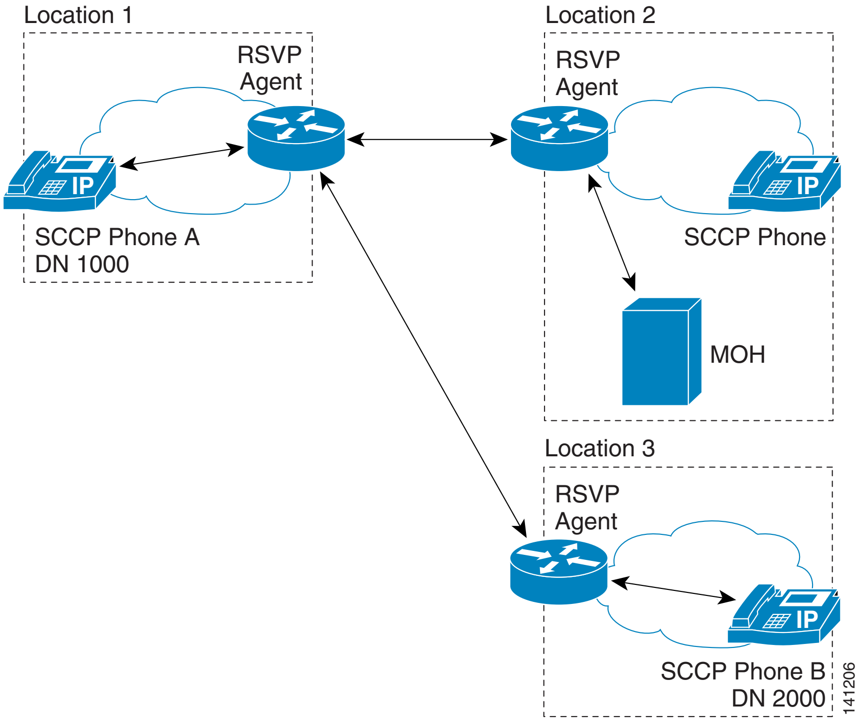
Figure 9-6 Phone B Puts Phone A on Hold, MOH Server in Same Location as Phone B



This example shows a phone call between phone A and phone B, with the Music On Hold server in the same location as phone B. If phone B puts phone A on hold, so phone A receives music on hold, the reservation that was used to connect phone A and phone B gets reused for the Music On Hold session. No additional reservation gets created.

Figure 9-7 shows a call that invokes Music On Hold. Phones A and B are in a call when phone B puts phone A on hold. In the illustration, the MOH server occupies a different location from both phone A and phone B. (Phone A, phone B, and the Music On Hold server each reside in a different location.)

Figure 9-7 Phone B Puts Phone A on Hold, MOH Server in a Third Location

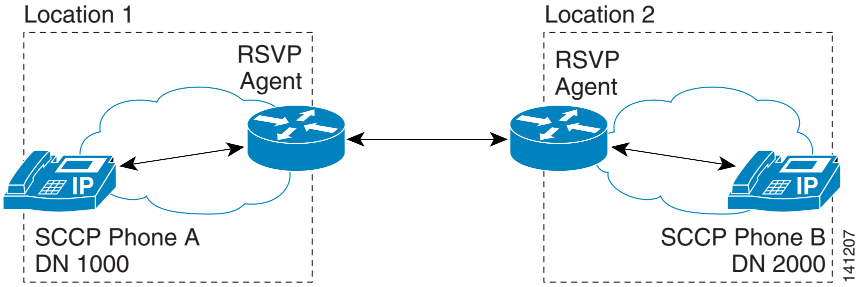


If phone B puts phone A on hold, so phone A receives music on hold, RSVP Agent preserves the reservation that was used to connect phone A and phone B. Another RSVP Agent creates a new reservation between phone A and the MOH server.

RSVP and Call Transfer

The following figures show RSVP interaction with a call-transfer scenario. Figure 9-8 shows the initial scenario, where phone A is in a call with phone B.

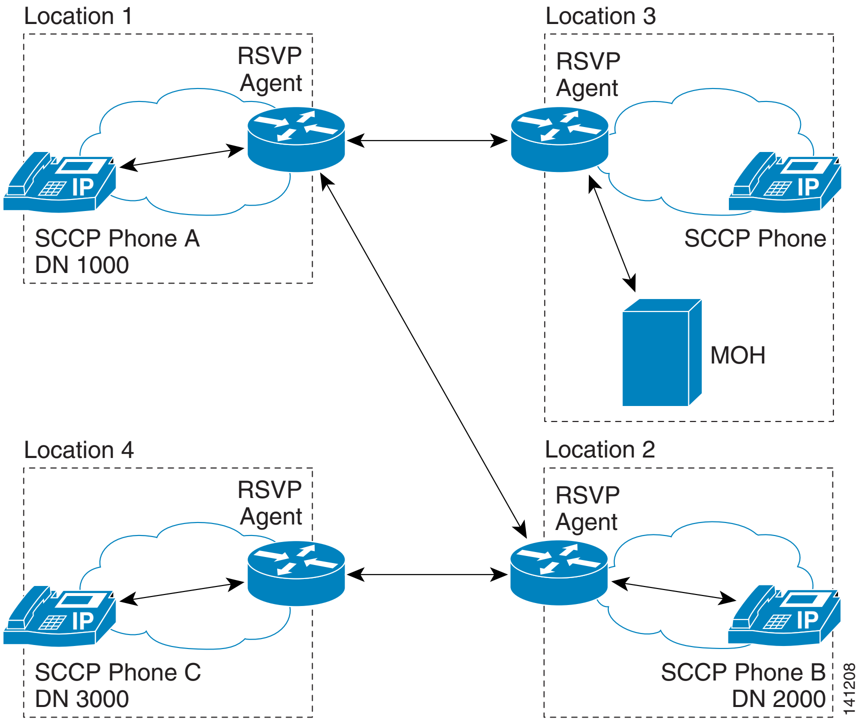
Figure 9-8 Call from Phone A to Phone B with RSVP Agent Connection



In the illustration, phone A, DN 1000, location 1, calls phone B, DN 2000, location 2. RSVP Agent establishes a reservation for the call. Phone B presses the Transfer button and dials DN 3000. Phone C, DN 3000, location 4, answers the call.

Figure 9-9 shows the RSVP connections as phone B transfers the call to phone C.

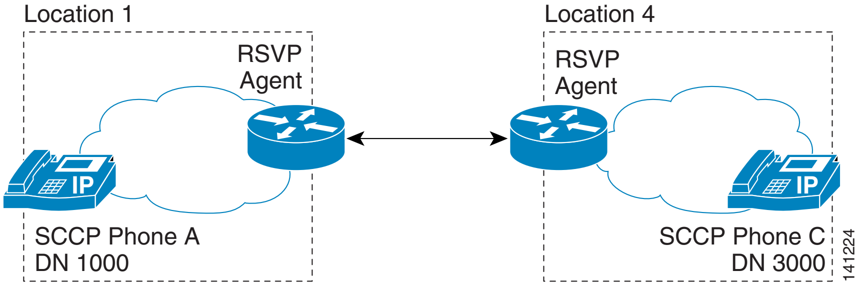
Figure 9-9 Phone B Initiates Transfer of Call from Phone A to Phone C



When phone B initiates transfer of the call from phone A to phone C in this configuration, the RSVP Agent preserves the reservation between phone A and phone B. An RSVP Agent creates a new RSVP reservation between phone A and the MOH server. An RSVP Agent creates a new reservation between phone B and phone C.

Figure 9-10 shows the scenario after the transfer completes.

Figure 9-10 Call Transfer Completes, and Phone A and Phone C Get Connected



After phone B completes the transfer, a new RSVP reservation gets created between phone A and phone C. The RSVP reservations between phone A and the MOH server, phone A and phone B, and phone B and phone C, all get torn down.

RSVP and MLPP

The following sections discuss various RSVP-based MLPP scenarios.

Scenario 1: A lower priority call gets preempted during congestion.

Initial call RSVP Policy: Mandatory

Mid-call RSVP Policy: Call fails. No retries

Other configuration details: RSVP bandwidth equals 100 kbps. Each call takes 80 kbps; therefore, only one call can obtain a reservation successfully.

1. Start a Priority call.

   The call succeeds.

2. Start a Routine call.

   The call fails to initialize due to the Mandatory setting.

3. Start a Flash call.

   The call succeeds because the Priority call gets preempted.

Scenario 2: A video call proceeds as an audio-only call if sufficient bandwidth does not exist.

Initial call RSVP Policy: Mandatory with video desired

Mid-call RSVP Policy: Best effort

Other configuration details: RSVP bandwidth equals 100 kbps. Each audio calls takes 80 kbps; therefore, only one call can obtain a reservation successfully.

1. Start a Priority audio call.

   The call succeeds.

2. Start a Flash video call.

   The call starts as audio only because insufficient bandwidth exists for a video call. The quality of the Priority call decreases.

Scenario 3: A lower priority call continues during congestion with no premium QoS.

Initial call RSVP Policy: Optional

Mid-call RSVP Policy: Best effort

Other configuration details: RSVP bandwidth equals 100 kbps. Each audio calls takes 80 kbps; therefore, only one call can obtain a reservation successfully.

1. Start a Priority call.

   The call succeeds.

2. Start a Routine call.

   The call succeeds, but no premium QoS is available. (The call uses a different DSCP.)

3. Start a Flash call.

   The call succeeds. The QoS for the Priority call decreases.

4. End (hang up) the Flash call.

   The Priority call recovers the RSVP reservation, and QoS increases.

Troubleshooting RSVP

RSVP provides the performance monitoring (PerfMon) counters, Call Detail Records (CDRs), alarms, and trace information to assist with troubleshooting RSVP. See the following topics:

- Performance Monitoring Counters, page 9-21
- Call Detail Records, page 9-21
- Alarms, page 9-22
- Trace Information, page 9-22

See the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide* for details.

Performance Monitoring Counters

The following Cisco Unified CallManager RSVP admission control performance monitoring counters exist:

- RSVP AudioReservationErrorCounts
- RSVP MandatoryConnectionsInProgress
- RSVP OptionalConnectionsInProgress
- RSVP TotalCallsFailed
- RSVP VideoCallsFailed
- RSVP VideoReservationErrorCounts

These location-based and node-based performance monitoring counters do not synchronize across nodes.

To troubleshoot RSVP Agent resources, the following RSVP performance monitoring counters exist:

- OutOfResources
- ResourceActive
- ResourceAvailable
- ResourceTotal

See the *Cisco Unified CallManager Serviceability System Guide* for descriptions of the performance monitoring counters. See the *Cisco Unified CallManager Serviceability Administration Guide* for instructions as to how to view performance monitoring counters.

Call Detail Records

The Cisco Unified CallManager Quality of Service (QoS) RSVP Agent feature adds the following Call Detail Record (CDR) fields:

- origRSVPAudioStat—Status of RSVP audio reservation from originator to terminator
- destRSVPAudioStat—Status of RSVP audio reservation from terminator to originator

- origRSVPVideoStat—Status of RSVP video reservation from originator to terminator
- destRSVPVideoStat—Status of RSVP video reservation from terminator to originator

These fields reflect the status of RSVP bandwidth reservation per audio or video stream.

The following values apply for the Cisco Unified CallManager RSVP CDR status fields:

- 0—Indicates RSVP NO RESERVATION condition, which is the default value.
- 1—Indicates RSVP RESERVATION FAILURE condition at call setup or feature invocation.
- 2—Indicates RSVP RESERVATION SUCCESS condition at call setup or feature invocation.
- 3—Indicates RSVP RESERVATION NO RESOURCE (RSVP Agent) condition at call setup or feature invocation.
- 4—Indicates RSVP MID_CALL FAILURE_PREEMPTED condition (preempted after call setup).
- 5—Indicates RSVP MID_CALL FAILURE_LOST_BANDWIDTH condition (includes all midcall failure except MLPP preemption).

The Cisco Unified CallManager RSVP CDR status field value gets concatenated, and the most recent 32 status values get retained for the call.

Example

A call establishes with the Optional RSVP policy, and the initial RSVP reservation succeeds. The call subsequently loses its bandwidth reservation and regains the bandwidth reservation after retrying. This sequence repeats several times during the call, and the call ends with a successful RSVP reservation. In this case, the CDR shows the following string as the Cisco Unified CallManager RSVP reservation status for that particular stream:

> “2:5:2:5:2:5:2” (success:lost_bw:success:lost_bw:success:lost_bw:success)

See *Cisco Unified CallManager Call Detail Record Definitions* for additional information.

Alarms

The RsvpNoMoreResourcesAvailable Cisco Unified CallManager Serviceability alarm gets generated when no RSVP Agent resource is available.

The following Cisco Unified CallManager alarm catalog defines this alarm: /vob/ccm/Common/XML/AlarmCatalog/CallManager.xml.

See the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide* for details.

Trace Information

RSVP generates several SDL and SDI Traces for the Cisco CallManager service upon RSVP reservation failure. The user sees the RSVP error codes in both the Cisco Unified CallManager SDL and SDI Trace files.

The RSVP Agent can send the following RSVP Reservation error codes:

- QOS_CAUSE_RESERVATION_TIMEOUT=0,
- QOS_CAUSE_PATH_FAIL,
- QOS_CAUSE_RESV_FAIL,

- QOS_CAUSE_LISTEN_FAIL,
- QOS_CAUSE_RESOURCE_UNAVAILABLE,
- QOS_CAUSE_LISTEN_TIMEOUT,
- QOS_CAUSE_RESV_RETRIES_FAIL,
- QOS_CAUSE_PATH_RETRIES_FAIL,
- QOS_CAUSE_RESV_PREEMPTION,
- QOS_CAUSE_PATH_PREEMPTION,
- QOS_CAUSE_RESV_MODIFY_FAIL,
- QOS_CAUSE_PATH_MODIFY_FAIL

See the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide* for details.

Where to Find More Information

Related Topics

- Call Admission Control, page 8-1
- Location Configuration, *Cisco Unified CallManager Administration Guide*
- Route Patterns, page 17-6
- Media Resource Group List Configuration, *Cisco Unified CallManager Administration Guide*
- Device Pool Configuration, *Cisco Unified CallManager Administration Guide*
- Region Configuration, *Cisco Unified CallManager Administration Guide*
- Route Pattern Configuration, *Cisco Unified CallManager Administration Guide*
- Gatekeeper Configuration, *Cisco Unified CallManager Administration Guide*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified IP Phones, page 43-1
- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*
- Understanding Video Telephony, page 44-1
- Trunk Configuration, *Cisco Unified CallManager Administration Guide*
- Multilevel Precedence and Preemption, *Cisco Unified CallManager Features and Services Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Call Detail Record Definitions*
- Cisco Multimedia Conference Manager (Command Reference) IOS documentation

CHAPTER 10

Cisco TFTP

The Cisco TFTP service builds and serves files that are consistent with the Trivial File Transfer Protocol (TFTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files.

A configuration file contains a prioritized list of Cisco Unified CallManagers for a device (SCCP and SIP phones and gateways), the TCP ports on which the device connects to those Cisco Unified CallManagers, and an executable load identifier. Configuration files for selected devices contain locale information and URLs for the phone buttons: messages, directories, services, and information. Configuration files for gateways contain all their configuration information.

Configuration files may be in a .cnf, a .cnf.xml, or an .xml format, depending on the device type and your TFTP service parameter settings. When you set the BuildCNFType service parameter to Build All, the TFTP server builds both .cnf.xml and .cnf format configuration files for all devices. When you set this service parameter to Build None, the TFTP server builds only .cnf.xml files for all devices. When this parameter is set to Build Selective, which is the default value, the TFTP server builds .cnf.xml files for all devices and, in addition, builds .cnf files only for a select list of device types that are provided in Table 10-1:

Table 10-1 Devices with Build Selective BuildCNFType

Device Type	Device Name
MODEL_30SPP	Cisco 30 SP+
MODEL_12SPP	Cisco 12 SP+
MODEL_12SP	Cisco 12 SP
MODEL_12S	Cisco 12 S
MODEL_30VIP	Cisco 30 VIP or DPA
MODEL_IP_CONFERENCE_PHONE	Cisco 7935
MODEL_SCCP_PHONE	SCCP Phone
MODEL_VEGA	Analog Access
MODEL_UONE	Voice Mail Port

This section describes the relationship among Cisco Unified CallManager, TFTP, and Dynamic Configuration Protocol (DHCP) as well as the relationship between devices and the TFTP server. This section contains the following topics:

- TFTP Process Overview for SCCP Devices, page 10-2
- TFTP Process Overview for Cisco SIP IP Phones, page 10-3

- Understanding How Devices Use DHCP and Cisco TFTP, page 10-4
- Understanding How Devices Access the TFTP Server, page 10-6
- Understanding How Devices Identify the TFTP Server, page 10-6
- Configuring a Backup or Fallback TFTP Server, page 10-7
- Centralized TFTP in a Multiple Cluster Environment, page 10-7
- Alternate TFTP Paths, page 10-8
- Configuration Tips for Centralized TFTP, page 10-9
- Customizing and Modifying Configuration Files, page 10-9
- TFTP Configuration Checklist, page 10-10
- Where to Find More Information, page 10-10

TFTP Process Overview for SCCP Devices

The TFTP server can handle simultaneous requests for configuration files. This section describes the request process.

When a device boots, it queries a DHCP server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. (Some devices, such as the Cisco Unified IP Phone 7960 model, support up to two TFTP servers. If the primary TFTP server is not reached, such devices attempt to reach the fallback TFTP server.)

Note If DHCP is not enabled on a device, you must assign it an IP address and configure the TFTP server locally on the device.

The device requests a configuration file from the TFTP server. The TFTP server searches an internal cache, then primary and alternate paths (if specified) for the configuration file. If the TFTP server finds the configuration file, it sends it to the device. If the device receives the Cisco Unified CallManager name, it resolves the name by using DNS and opens a Cisco Unified CallManager connection. If the device does not receive an IP address or name, it uses the default server name.

If the TFTP server cannot find the configuration file, it sends a “file not found” error message to the device.

Devices that are requesting a configuration file while the TFTP server is rebuilding configuration files or while processing the maximum number of requests receive a message from the TFTP server, which causes the device to request the configuration file later. The Maximum Serving Count service parameter, which can be configured, specifies 200 as the maximum number of requests.

For a more detailed description of how devices boot, see the “Understanding How Devices Use DHCP and Cisco TFTP” section on page 10-4.

TFTP Process Overview for Cisco SIP IP Phones

Unlike SCCP phones, SIP phones get all of their configurations from the TFTP server. From initial startup, the SIP phone contacts the configured TFTP server (either manually configured or configured through the DHCP server) to get the configuration files; it then registers itself to its configured Cisco Unified CallManager.

When the SIP phone configuration gets changed, the Cisco Unified CallManager database notifies the TFTP server to rebuild all of the configuration files or to rebuild selectively. The TFTP server retrieves information from the Cisco Unified CallManager database and converts it into the proper output format, according to the device type, and saves the output either in TFTP cache or on the disk.When the TFTP server gets a request, it searches either the cache or hard disk to serve the requested configuration file or default files.

The TFTP support for SIP phones builds and serves different formats of SIP configuration files from the Cisco Unified CallManager database for the following Cisco SIP IP Phones:

- Cisco Unified IP Phone 7970/71, 7961, 7941, 7911 (These phones share the same SIP configuration file format.)
- Cisco Unified IP Phone 7960, 7940 (These phones share the same SIP configuration file format.)
- Cisco Unified IP Phone 7905, 7912
- SIP dial plans on the preceding phone models
- Softkey templates on the preceding phone models

The TFTP server generates the following files from the Cisco Unified CallManager database for SIP phone configuration:

- Systemwide default configuration files and per-device configuration files.
- List of systemwide dial plans for Cisco Unified IP Phones 7970/71, 7960/61, 7940/41, and 7911.
- List of systemwide softkey template files.

The following configuration files get generated based on the SIP phone type.

Table 10-2 SIP Configuration Files That the TFTP Server Generates

SIP Configuration File Type	Model 7970/71, 7961, 7941, 7911	Model 7960/40	Model 7905	Model 7912
SIP IP Phone	SEP<mac>.cnf.xml	SIP<mac>.cnf	ld<mac>	gk<mac>
Dial Plan	DR<dialplan>.xml	<dialplan>.xml	Parameter in ld<mac>	Parameter in gk<mac>
Softkey Template	SK<softkey_template>.xml	Not configurable	Not configurable	Not configurable

The system derives filenames from the MAC Address and Description fields in the Phone Configuration window of Cisco Unified CallManager Administration and the devicename field in the Cisco Unified CallManager database. The MAC address uniquely identifies the phone.

SIP Phone Configuration Sequence

The SIP phone configuration sequence performs the following steps:

1. The administrator makes a change to the SIP phone (for example, by using either Phone Configuration, SIP Profile Configuration, or SIP Security Configuration in Cisco Unified CallManager Administration) and initiates a restart or reset of the phone.

2. The Cisco Unified CallManager database sends a change notification to the TFTP server and to Cisco Unified CallManager.
3. Upon notification (either automatically or by the administrator or user resetting or restarting the phone), Cisco Unified CallManager notifies the phone to get the configuration files again. The TFTP server then rebuilds all the configuration files for the selected phone. The configuration file name and format depend on the device type and protocol (see Table 10-2).
4. The SIP phone requests the configuration files from the TFTP server.
5. After getting the necessary configuration files, the phone registers its configured lines with Cisco Unified CallManager.

SIP Phone Dial Plan Configuration Sequence

The SIP phone dial plan configuration sequence performs the following steps:

1. The administrator configures the SIP dial plan and associates the dial plan with the SIP phone.
2. The Cisco Unified CallManager database sends a change notification to the TFTP server, which triggers the TFTP server to build a new set of files for the SIP phone.
3. The TFTP server rebuilds the Dial Plan configuration file and/or the configuration file for the SIP phone.
4. When all the updates to the dial rules have been made to the Cisco Unified CallManager database, the administrator clicks the Reset or Restart button to apply the change to the phone.

SIP Phone Softkey Template Configuration Sequence

The SIP phone softkey template configuration sequence performs the following steps:

1. The administrator configures the SIP softkey template and associates the softkey template with the SIP phone.
2. The Cisco Unified CallManager database sends a change notification to the TFTP server, which triggers the TFTP server to build a new set of files for the SIP phone.
3. The TFTP server rebuilds the softkey template configuration file and/or the configuration file for the SIP phone.
4. When all the updates to the softkeys have been made to the Cisco Unified CallManager database, the administrator presses the Reset or Restart button to apply the change to the phone.

Interaction with Cisco Extension Mobility

When a user logs in to a device by using Cisco Extension Mobility, the Cisco Unified CallManager database notifies the TFTP server to rebuild the SEP<mac>.cnf.xml file to include the new dial plan filenames that are defined for the lines on the device profile.

Serviceability Counters

The TFTP server provides counters in Cisco Unified CallManager Serviceability for troubleshooting purposes. See the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide* for more information.

Understanding How Devices Use DHCP and Cisco TFTP

Cisco telephony devices require IP addresses that are assigned manually or by using DHCP. Devices also require access to a TFTP server that contains device loads and device configuration files.

Obtaining an IP Address

If DHCP is enabled on a device, DHCP automatically assigns IP addresses to the device when you connect it to the network. The DHCP server directs the device to a TFTP server (or to a second TFTP server, if available for the device). For example, you can connect multiple Cisco Unified IP Phones anywhere on the IP network, and DHCP automatically assigns IP addresses to them and provides them with the path to the appropriate TFTP server.

If DHCP is not enabled on a device, you must assign it an IP address and configure the TFTP server locally on the device.

The default DHCP setting varies depending on the device:

- Cisco Unified IP Phones stay DHCP-enabled by default. If you are not using DHCP, you need to disable DHCP on the phone and manually assign it an IP address.
- DHCP remains always enabled for Cisco Access Analog and Cisco Access Digital Gateways.
- For Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Modules, the Network Management Processor (NMP) on the Cisco Catalyst 6000 may or may not have DHCP enabled. If DHCP is not enabled, you will need to configure the IP address through the Cisco CATOS command-line interface on the Cisco Catalyst 6000.

Requesting the Configuration File

After a device obtains an IP address (through DHCP or manual assignment), it requests a configuration file from the TFTP server.

If a device has been manually added into the Cisco Unified CallManager database, the device accesses a configuration file that corresponds to its device name. If a phone is not manually configured and auto-registration is enabled, the phone requests a default configuration file from the TFTP server and starts the auto-registration procedure with Cisco Unified CallManager.

Note Phones represent the only device type that can auto-register and that have default configuration files. You must manually add all other devices to the Cisco Unified CallManager database.

If a phone has an XML-compatible load, it requests a .cnf.xml format configuration file; otherwise, it requests a .cnf file.

Note When you set the BuildCNFType service parameter to Build All, the TFTP server builds both .cnf.xml and .cnf format configuration files for all devices. When you set this service parameter to Build None, the TFTP server builds only .cnf.xml files for all devices. When this parameter is set to Build Selective, which is the default value, the TFTP server builds .cnf.xml files for all devices and, in addition, builds .cnf files only for a select list of devices that do not support .cnf.xml. Table 10-1 provides a list of these devices.

Contacting Cisco Unified CallManager

After obtaining the configuration file from the TFTP server, a device attempts to make a TCP connection to the highest priority Cisco Unified CallManager in the list that is specified in the configuration file. If the device was manually added to the database, Cisco Unified CallManager identifies the device. If auto-registration is enabled in Cisco Unified CallManager, phones that were not manually added to the database attempt to auto-register in the Cisco Unified CallManager database.

Cisco Unified CallManager informs devices that are using .cnf format configuration files of their load ID. Devices that are using .xml format configuration files receive the load ID in the configuration file. If the device load ID differs from the load ID that is currently executing on the device, the device requests the load that is associated with the new load ID from the TFTP server and resets itself. For more information on device loads, refer to the "Device Support" section on page 11-1.

After a telephone is ready to make a call, it will request an available ringer list from the TFTP server. If the telephone user changes the ring type, the TFTP server sends the new ring type.

Understanding How Devices Access the TFTP Server

You can enable the IP phones and gateways to discover the TFTP server IP address in one or more of the following ways, depending on the device type:

- Gateways and phones can use DHCP custom option 150.

  Cisco recommends this method. With this method, you configure the TFTP server IP address as the option value.
- Gateways and phones can use DHCP option 066.

  You may configure either the host name or IP address of the TFTP server as the option value.
- Gateways and phones can query CiscoCM1.

  Ensure the Domain Name System (DNS) can resolve this name to the IP address of the TFTP server. Cisco does not recommend this option because it does not scale.
- You can configure phones with the IP address of the TFTP server. If DHCP is enabled on the phone, you can still configure an alternate TFTP server IP address locally on the phone that will override the TFTP address that was obtained through DHCP.
- Gateways and phones also accept the DHCP Optional Server Name (sname) parameter.
- The phone or gateway can use the value of Next-Server in the boot processes (siaddr).

Devices save the TFTP server address in nonvolatile memory. If one of the preceding methods was available at least once, but is not currently available, the device uses the address that is saved in memory.

You can configure the TFTP service on the first node or a subsequent node, but usually you should configure it on the first node. For small systems, the TFTP server can coexist with a Cisco Unified CallManager on the same server.

Understanding How Devices Identify the TFTP Server

Phones and gateways use an order of precedence for selecting the address of the TFTP server if they receive conflicting or confusing information from the DHCP server. The basis for the order of precedence depends on the method that is used to specify the TFTP server (method 1 in the following list has the highest precedence):

1. The phone or Catalyst 6000 gateway uses a locally configured TFTP server address.

   This address overrides any TFTP address that the DHCP server sends.
2. The phone or gateway queries the DNS name CiscoCM1, and it is resolved.

   The phone or gateway always tries to resolve the DNS name CiscoCM1. If this name is resolved, it overrides all information that the DHCP server sends.

You do not need to name the TFTP server CiscoCM1, but you must enter a DNS CName record to associate CiscoCM1 with the address or name of the TFTP server. Cisco does not recommend this option because it does not scale.

3. The phone or gateway uses the value of Next-Server in the boot processes.

   The address of the TFTP server traditionally uses this DHCP configuration parameter. When BOOTP servers are configured, this field typically serves as the address of the TFTP server.

   This information gets returned in the siaddr (server IP address) field of the DHCP header. Use this option, if available, because some DHCP servers will place their own IP address in this field when it is not configured.

4. The phone or gateway uses the site-specific option 150.

   This option resolves the issue that some servers do not allow the Next-Server configuration parameter. Some servers allow access to the Next-Server parameter only when IP addresses are statically assigned.

5. The phone or gateway uses the Optional Server Name parameter.

   This DHCP configuration parameter designates the host name of a TFTP server. Currently, you can configure only a host name in this parameter; do not use a dotted decimal IP address.

6. The phone or gateway uses the 066 option, which is the name of the boot server.

   Option 066 normally replaces the sname (server name) field when option overloading occurs. This name field can contain a host name or a dotted decimal IP address.

   Do not use the 066 option with the 150 option.

   The device prefers the IP address over the name that is given by the 066 option if they are sent together. If both a dotted decimal IP address and a 150 option are sent, order of preference depends on the order in which they appear in the option list. The device chooses the last item in the option list because option 066 and option 150 remain mutually exclusive.

Configuring a Backup or Fallback TFTP Server

You should configure only one TFTP server in a cluster unless you want to have a backup or a fallback TFTP server. If a device (phone or gateway) gets no response from the first TFTP server and if a fallback TFTP server is configured, the device will try to connect to the second TFTP server. The fallback TFTP server gets configured by option 150 in DHCP to a list of two TFTP servers in the same cluster.

Centralized TFTP in a Multiple Cluster Environment

A Centralized TFTP server supports multiple clusters within one large campus environment. The Centralized TFTP server design allows phones to be moved from one building to another within a campus. It also supports a mixed OS multicluster environment.

Devices that are registered and configured in any cluster can home into a single TFTP server (Centralized TFTP server) that will then serve files to those devices. The following sections describe how the Centralized TFTP server works in a Cisco Unified CallManager multicluster environment:

- Master Centralized TFTP Server, page 10-8
- Sending Files to the Master Centralized TFTP Server, page 10-8

- Alternate TFTP Paths, page 10-8
- Configuration Tips for Centralized TFTP, page 10-9

Master Centralized TFTP Server

You can configure a single TFTP server to build the configuration files for devices in its cluster, to serve all security, firmware, and configuration files to those devices. This single server, a Master Centralized Server, serves files from all the other Cisco Unified CallManager clusters. The centralized TFTP server in the other clusters will build files only for devices that are configured for that particular cluster. All endpoint requests get sent to the master centralized TFTP server, either by hard coding or by DHCP configuration at the endpoint.

The master centralized TFTP queries files from other centralized TFTP servers if the requested file(s) is not found in the local cache of the master centralized TFTP server. When the master centralized TFTP server receives a file request, it looks first in the local cache for the requested file. If the file does not exist there, then the master centralized TFTP server will request the file from the other configured centralized TFTP servers. The request will eventually time out, if the response is not received within a set amount of time.

Sending Files to the Master Centralized TFTP Server

When an off-cluster server receives a request from the master centralized TFTP server, it searches for the file and, if found, sends the requested file back to the master centralized TFTP server. The master centralized TFTP server then sends the requested file to the device that originally requested the file, by using TFTP. Should the off-cluster server not have the requested file, it will respond to the master centralized TFTP server with “File Not Found” (HTTP Error 404), and the master centralized TFTP server continues the process with the next off-cluster server until either the file is located or no remaining options exist.

The off-cluster server indicates to the master centralized TFTP server, by using an HTTP Error 503 that it is busy and that the master centralized TFTP server should try the request again later. This message will also get sent to the endpoint device that made the original request.

Alternate TFTP Paths

You can specify alternate TFTP paths if you have multiple clusters, if you want to configure only one server for many DHCP scopes, or you want to have one DHCP scope. You can specify up to 10 alternate servers by entering a value in any of the Alternate Cisco File Server fields of the Cisco TFTP service parameter. For more information on service parameters, refer to the “Service Parameters Configuration” chapter in the *Cisco Unified CallManager Administration Guide*.

You can use either of the following syntax examples:

- host://<IP of the off-cluster TFTP server> (for example, host://10.10.134.24)
- HOST://<IP of the off-cluster TFTP server> (for example, HOST://10.10.134.24)

If DNS is also supported, you can also use one of the following syntax examples:

- HOST://<name of the off-cluster TFTP server> (for example, HOST://tftp-prim)
- HOST://<name of the off-cluster TFTP server> (for example, HOST://tftp-second)

You cannot use any other syntax.

The primary TFTP server should have the Alternate Cisco File Server (1 to 10) values set for external Cisco Unified CallManager clusters. The primary TFTP server serves configuration files from these servers for phones and devices in the external clusters. To avoid creating a loop, ensure that the TFTP servers on the external clusters do not point to each other.

Configuration Tips for Centralized TFTP

The following list comprises tips to remember when you are configuring a centralized TFTP server:

- You should configure only the master centralized TFTP server with alternate file locations that are specified in its list. Off-cluster TFTP servers should have no alternate file locations. See the "Alternate TFTP Paths" section on page 10-8. Refer to "Service Parameters Configuration" in the *Cisco Unified CallManager Administration Guide* for information on how to configure the TFTP service.
- You can configure 1 to 10 Alternate Cisco File Servers in the Cisco TFTP Service Parameters Configuration window. If Alternate Cisco File Server 1 contains an empty parameter value, TFTP will stop searching for alternate servers. For example, if Alternate Cisco File Servers 2 through 10 are configured and 1 is empty, and TFTP is searching for servers, it will not search Alternate Cisco File Servers 2 through 10.
- When phones are configured in a Cisco Unified CallManager other than the cluster where the master centralized TFTP server is configured and auto-registration is enabled, and the off-cluster Cisco Unified CallManager goes down, if the phones are configured to submit a request from the centralized TFTP server, they may inadvertently get auto-registered on the central Cisco Unified CallManager. Therefore, you should disable auto-registration if it is not already disabled or delete the inadvertently registered phone after making sure that the cluster to which it belongs is up and running.

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 Unified Communications Platform Administration, from the TFTP Server File Upload page. Refer to the *Cisco Unified Communications Operating System Administration Guide* for information on how to upload files to the TFTP folder on a Cisco Unified CallManager server.

TFTP Configuration Checklist

Table 10-3 lists the steps that are needed to configure the Cisco TFTP service.

Table 10-3 TFTP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Activate and start the Cisco TFTP service on the appropriate server.	*Cisco Unified CallManager Serviceability Administration Guide*
Step 2	Configure the appropriate service parameters, including the Alternate File Location parameters, if appropriate.	Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	If you change a non-configuration file such as a load file or RingList.xml, start and stop the Cisco TFTP service or set the service parameter, Enable Caching of Constant and Bin Files at Startup TFTP, to True (if it is already set to True, set to False, click **Update**, set to True again, and click **Update**). **Note** You must upload files to the TFTP directory from Cisco Unified Communications Platform Administration. Refer to the *Cisco Unified Communications Operating System Administration Guide* for more information.	*Cisco Unified CallManager Serviceability Administration Guide* Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topic

- SIP Dial Rules, page 19-4
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
- DHCP Subnet Configuration, *Cisco Unified CallManager Administration Guide*
- DHCP Server Configuration, *Cisco Unified CallManager Administration Guide*
- SIP Dial Rules Configuration, *Cisco Unified CallManager Administration Guide*
- SIP Profile Configuration, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified Communications Operating System Administration Guide*

Device Support

This section provides general information about how Cisco Unified CallManager interacts with Cisco Unified Communications devices in your network and covers the following topics:

- Supported Devices, page 11-1
- Device Configuration Files, page 11-2
- Device Firmware Loads, page 11-2
- Device Pools, page 11-3
- Call Preservation, page 11-4
- Where to Find More Information, page 11-6

Supported Devices

The Cisco Unified CallManager supports many types of devices, including those in the following list:

- Cisco Unified IP Phones
- Analog gateway ports
- T1 gateway
- E1 gateway
- Transcoding resource
- Software Media Termination Point (MTP)
- Annunciator
- Conference resource (hardware)
- Conference resource (software)
- CTI port (TAPI and JTAPI)
- Cisco SoftPhone
- Messaging (voice mail)
- Intercluster trunk
- SIP trunks
- Video inputs

Device Configuration Files

The Cisco Trivial File Transfer Protocol (Cisco TFTP), a Windows 2000 service, builds configuration files from information that is found in the Cisco Unified CallManager database.

The device-specific configuration files use the name format SEP, SAA, SDA, CFB, VGC, or MTP + MAC address:

- SEP—Selsius Ethernet Phone (Cisco IP Phone model 12 SP+, Cisco IP Phone model 30 VIP, Cisco Unified IP Phone 7902, Cisco Unified IP Phone 7905, Cisco Unified IP Phone 7910, Cisco Unified IP Phone 7912, Cisco Unified IP Phone 7920, Cisco Unified IP Phone 7935, Cisco Unified IP Phone 7936, Cisco Unified IP Phone 7940, Cisco Unified IP Phone 7960, and Cisco Unified IP Phone 7970)
- SAA—Selsius Analog Access (Cisco Catalyst 6000 24 Port FXS Analog Interface Module)
- SDA—Selsius Digital Access (DT-24+, DE-30+, Cisco Catalyst 6000 8 Port Voice E1/T1)
- VGC—Cisco VG248 Analog Phone Gateway (Cisco VG248 ports and units appear as distinct devices in the same Cisco Unified CallManager. All 48 device ports register within the same Cisco Unified CallManager cluster as device type "Cisco VGC Phone.")
- MTP—Media Termination Point

Configuration files also contain a list of Cisco Unified CallManagers in priority order. Network addresses comprise either the fully qualified domain name, for example, "cm1.cisco.com," or dotted IP address "172.116.21.12" plus a TCP port. See the "Cisco TFTP" section on page 10-1 for more information.

When a device needs to get its configuration file, the device sends a TFTP request for the device-specific configuration filename.

Note You can specify button URLs in device configuration for Cisco Unified IP Phone Models 7970, 7960, and 7940. If the URL is blank, Cisco Unified CallManager uses the enterprise values. Refer to the "Enterprise Parameters Configuration" section in the *Cisco Unified CallManager Administration Guide*.

Device Firmware Loads

Loads comprise files that contain updated firmware for devices. Four types of firmware loads exist: phone loads, gateway loads, MTP loads, and conference bridge loads. During installation or upgrade, Cisco Unified CallManager provides the latest loads; however, you can also receive a load between releases that can contain patches or other information that is important to the devices that use loads, such as phones or gateways.

The /usr/local/cm/tftp subdirectory stores these load files as *.bin, .zup, or .sbin files; for example, D501A022.bin. During installation or upgrade, this location stores the latest loads. You must copy new loads that you receive between releases to this location for the system to access them.

The Loads Table contains the most current information on load descriptions for each device type.

Updating Device Loads

You can apply a new load to a single device before applying it as a systemwide default. This method can prove useful for testing purposes. Remember, however, that only the device that you have updated with the new load will use that load. All other devices of that type use the old load until you update the systemwide defaults for that device with the new load.

Device Pools

Device pools scale and simplify the distribution of Cisco Unified CallManager redundancy groups. A device pool allows the following primary attributes to be assigned globally to a device:

- Cisco Unified CallManager Group—This group specifies a list of up to three Cisco Unified CallManagers, which can be used for call processing in a prioritized list.
- Date/Time Group—Date/Time group specifies the date and time zone for a device.
- Region—You require regions only if multiple voice codecs are used within an enterprise. Regions define the voice codecs that are used within and between regions.
- Softkey Template—Assign specific softkey templates to device pools and then assign the device pool to users who require the template.
- SRST Reference—Disable or use default gateway for SRST.

Optional calling search space can prevent rogue installations of IP phones on your network. For example, rogue phones that are plugged into the network autoregister in a device pool that has a calling search space that is restricted only to the Cisco Unified CallManager administrator. This search space can have a Primary Line Automatic Ringdown that is assigned to it, so, when the user goes off hook, the call immediately connects to security or the Cisco Unified CallManager administrator.

Typically, the following scenario applies with respect to configuring device pools. The deployment model drives the exact model of clustering and device pools that are used:

- Redundancy for single-site cluster, multisite WAN centralized call processing, and multisite WAN distributed call processing—Device pool configuration uses Cisco Unified CallManager groups as redundancy basis. For example, a cluster can have up to eight Cisco Unified CallManager servers: A, B, C, D, E, F, G, and H; four configured as active and four configured as backup. Using 1:1 redundancy, the groups would comprise servers AB, CD, EF, and GH. Using 1:1 redundancy with load balancing, the groups would comprise AB, BA, CD, DC, EF, FE, GH, and HG.

Note A Cisco Unified CallManager cluster with more than 20,000 IP phones requires 1:1 redundancy. You may also configure 2:1 redundancy for smaller clusters; for example, AC, BC, DF, and EF, where ABDE comprise primary servers, and CF comprise the backup servers.

- Region requirements for single-site cluster—This scenario does not require use of regions because all calls use the G.711 codec for calls.
- Region requirements for multisite WAN centralized and distributed call processing—Each cluster could potentially have a G.711 and G.729 region per Cisco Unified CallManager redundancy group.
- Total device pools = Number of sites x regions.

  Total device pools = Regions x Cisco Unified CallManager redundancy groups.

Refer to the "Device Pool Configuration" section in the *Cisco Unified CallManager Administration Guide* for information on how to configure device pools.

Call Preservation

The call preservation feature of Cisco Unified CallManager ensures that an active call will not be interrupted when a Cisco Unified CallManager fails or when communication fails between the device and the Cisco Unified CallManager that set up the call.

Cisco Unified CallManager supports full call preservation for an extended set of Cisco Unified Communications devices. This support includes call preservation between Cisco Unified IP Phones, Media Gateway Control Protocol (MGCP) gateways that support Foreign Exchange Office (FXO) (non-loop-start trunks) and Foreign Exchange Station (FXS) interfaces, and, to a lesser extent, conference bridge, MTP, and transcoding resource devices.

The following devices and applications support call preservation. If both parties connect through one of the following devices, Cisco Unified CallManager maintains call preservation:

- Cisco Unified IP Phones
- Software conference bridge
- Software MTP
- Hardware conference bridge (Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module, Cisco Catalyst 4000 Access Gateway Module)
- Transcoder (Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module, Cisco Catalyst 4000 Access Gateway Module)
- Non-IOS MGCP gateways (Catalyst 6000 24 Port FXS Analog Interface Module, Cisco DT24+, Cisco DE30+, Cisco VG200)
- Cisco IOS MGCP Gateways (Cisco VG200, Catalyst 4000 Access Gateway Module, Cisco 2620, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3810)
- Cisco VG248 Analog Phone Gateway
- Cisco Unified CallManager Attendant Console

The following devices and applications do not support call preservation in this release:

- Annunciator
- H323 devices
- CTI applications
- TAPI applications
- JTAPI applications

Call Preservation Scenarios

Table 11-1 lists and describes how call preservation is handled in various scenarios.

Table 11-1 Call Preservation Scenarios

Scenario	Call Preservation Handling
Cisco Unified CallManager fails.	A Cisco Unified CallManager failure causes the call-processing function for all calls that were set up through the failed Cisco Unified CallManager to be lost. The affected devices recognize that their current Cisco Unified CallManager failed. Similarly, the other Cisco Unified CallManagers in the cluster detect the Cisco Unified CallManager failure. Cisco Unified CallManager maintains affected active calls until the end user hangs up or until the devices can determine that the media connection has been released. Users cannot invoke any call-processing features for calls that are maintained as a result of this failure.
Communication failure occurs between Cisco Unified CallManager and device.	When communication fails between a device and the Cisco Unified CallManager that controls it, the device recognizes the failure and maintains active connections. The Cisco Unified CallManager recognizes the communication failure and clears call-processing entities that are associated with calls in the device where communication was lost. The Cisco Unified CallManagers still maintain control of the surviving devices that are associated with the affected calls. Cisco Unified CallManager maintains affected active calls until the end user hangs up or until the devices can determine that the media connection has been released. Users cannot invoke any call-processing features for calls that are maintained as a result of this failure.
Device failure (Phone, gateway, conference bridge, transcoder, MTP)	When a device fails, the connections that exist through the device stop streaming media. The active Cisco Unified CallManager recognizes the device failure and clears call-processing entities that are associated with calls in the failed device. The Cisco Unified CallManagers maintain control of the surviving devices that are associated with the affected calls. Cisco Unified CallManager maintains the active connections (calls) that are associated with the surviving devices until the surviving end users hang up or until the surviving devices can determine that the media connection has been released.

Table 11-1 Call Preservation Scenarios (continued)

Scenario	Call Preservation Handling
Cisco Unified CallManager Attendant Console	Call preservation does not apply for Computer Telephony Integration (CTI) route point devices because a call is only accepted for redirect. If a Cisco Unified CallManager goes down before the call is extended to Telephony Call Dispatcher (TCD), the call does not transfer to TCD. If the Cisco Unified CallManager goes down before the call arrives at a phone after TCD redirects the call, the call will be lost. The attendant console inherits call preservation from the phone because it is a third-party control for a phone. Any active calls continue after Cisco Unified CallManager goes down, but calls on hold do not. The attendant console only supports call preservation via the associated phone.

Where to Find More Information

Related Topics

- Cisco TFTP, page 10-1
- Understanding Cisco Unified CallManager Voice Gateways, page 39-1
- Cisco Unified IP Phones, page 43-1

Additional Cisco Documentation

- Device Defaults Configuration, *Cisco Unified CallManager Administration Guide*
- Device Pool Configuration, *Cisco Unified CallManager Administration Guide*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified CallManager Group Configuration, *Cisco Unified CallManager Administration Guide*
- Date/Time Group Configuration, *Cisco Unified CallManager Administration Guide*

CHAPTER 12

Autoregistration

Autoregistration automatically assigns directory numbers to new devices as they connect to the IP telephony network. This section covers the following topics:

- Understanding Autoregistration, page 12-1
- Autoregistration Configuration Checklist, page 12-3
- Autoregistration with Multiple Protocol Support, page 12-2
- Where to Find More Information, page 12-4

Understanding Autoregistration

Use autoregistration if you want Cisco Unified CallManager automatically to assign directory numbers to new phones when you plug these phones in to your network. Cisco recommends you use autoregistration to add less than 100 phones to your network.

Cisco Unified CallManager disables autoregistration by default to prevent unauthorized connections to your network. Do not enable autoregistration unless you know what your dial plan looks like, including calling search spaces and partitions.

Caution Enabling autoregistration carries a security risk in that “rogue” phones can automatically register with Cisco Unified CallManager. You should enable autoregistration only for brief periods when you want to perform bulk phone adds.

Configuring mixed-mode, clusterwide security through the Cisco CTL client automatically disables autoregistration. If you want to use autoregistration and you have configured security, you must change the clusterwide security mode to nonsecure through the Cisco CTL client.

Another strategy for preventing unauthorized phones from connecting to your network entails creating a Rogue device pool that allows only 911 (emergency) and 0 (operator) calls. This device pool allows phones to register but limits them to emergency and operator calls. This device pool prevents unauthorized access to phones that continuously boot in an attempt to register in your network.

When you enable autoregistration, you specify a range of directory numbers that Cisco Unified CallManager can assign to new phones as they connect to your network. As new phones connect to the network, Cisco Unified CallManager assigns the next available directory number in the specified range. After a directory number is assigned to an autoregistered phone, you can move the phone to a new location, and its directory number remains the same. If all the autoregistration directory numbers are consumed, no additional phones can autoregister with Cisco Unified CallManager.

The Cisco Unified CallManager Group that has the Auto-registration Cisco Unified CallManager Group check box checked, specifies the list of Cisco Unified CallManagers that the phone will use to attempt to auto register. At least one Cisco Unified CallManager must be selected in the group. The first Cisco Unified CallManager in the selected list must also have the Auto-registration Disabled on this Cisco Unified CallManager check box unchecked in the Cisco Unified CallManager Configuration window. This ensures that the Cisco Unified CallManager allows the autoregistration request from the phone.

New phones auto-register with the primary Cisco Unified CallManager in the Cisco Unified CallManager group that has enabled the Auto-Registration Cisco Unified CallManager Group setting. That Cisco Unified CallManager automatically assigns each auto-registered phone to a default device pool based on the device type (refer to the "Device Defaults Configuration" chapter in the *Cisco Unified CallManager Administration Guide*). After a phone auto-registers, you can update its configuration and assign it to a different device pool and a different Cisco Unified CallManager (see the "Device Pools" section on page 5-10).

Autoregistration with Multiple Protocol Support

Autoregistration means that unknown phones will be coming into the network. Because the phones are unknown, Cisco Unified CallManager does not know whether the new phones should be registered as SIP phones or as SCCP phones. Therefore, the system administrator uses Cisco Unified CallManager Administration to specify the default protocol that new phones should use for autoregistration.

Cisco devices that support both SIP and SCCP protocols (Cisco Unified IP Phone models 7905, 7911, 7912, 7940, 7941, 7960, 7961, 7970, and 7971) will auto register with the protocol that is specified in the Auto Registration Phone Protocol Enterprise Parameter. Cisco devices that only support a single protocol will auto register with that protocol regardless of the Auto Registration Phone Protocol setting. For example, the Cisco Unified IP Phone 7902 only supports SCCP. If a Cisco Unified IP Phone 7902 auto registers, it will use the SCCP protocol regardless of whether the Auto Registration Phone Protocol is set to SIP.

Note To ensure that autoregistration works correctly, the Device Defaults Configuration window must have the correct phone image names specified for SIP and SCCP protocols.

To deploy phones in a mixed-protocol environment, you must perform additional steps when autoregistering a new mixed batch of phones. The first step requires that the administrator set the Cisco Unified CallManager Auto Registration Phone Protocol parameter in the Enterprise Parameters Configuration window to SCCP and install all the SCCP phones. The second step requires that the administrator change the Auto Registration Phone Protocol parameter to SIP and autoregister all the SIP phones.

Autoregistration Configuration Checklist

Table 12-1 lists general steps and guidelines for using autoregistration.

Table 12-1 Autoregistration Configuration Checklist

Configuration Steps		Procedures and related topics
Step 1	In the Enterprise Parameters Configuration window, set the Auto Registration Phone Protocol to SIP or SCCP. SCCP acts as the default, so change this setting when auto registering SIP phones.	Enterprise Parameters Configuration, *Cisco Unified CallManager Administration Guide*
Step 2	Configure only one Cisco Unified CallManager in the cluster to use for autoregistration. Always enable or disable autoregistration on this Cisco Unified CallManager only. If you want to shift the autoregistration function to another Cisco Unified CallManager in the cluster, you must reconfigure the appropriate Cisco Unified CallManagers, the Default Cisco Unified CallManager Group, and, possibly, the default device pools.	Cisco Unified CallManager Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Configure the Default Cisco Unified CallManager Group, or another Cisco Unified CallManager Group, as the autoregistration group. Choose the autoregistration Cisco Unified CallManager from Step 1 as the primary Cisco Unified CallManager in this group.	Cisco Unified CallManager Groups, page 5-3 Cisco Unified CallManager Group Configuration, *Cisco Unified CallManager Administration Guide*
Step 4	Configure a calling search space specifically for auto-registration. For example, you can use the auto-registration calling search space to limit auto-registered phones to internal calls only.	Partitions and Calling Search Spaces, page 15-1 Calling Search Space Configuration, *Cisco Unified CallManager Administration Guide*
Step 5	Configure the Default device pool for autoregistration by assigning the Default Cisco Unified CallManager Group and autoregistration calling search space to it. If you are configuring a separate default device pool for each device type, assign the default device pools to the device by using the Device Defaults Configuration window.	System-Level Configuration Settings, page 5-1. Device Pool Configuration, *Cisco Unified CallManager Administration Guide* Device Defaults Configuration, *Cisco Unified CallManager Administration Guide*
Step 6	Enable auto-registration only during brief periods when you want to install and autoregister new devices (preferably when overall system usage is at a minimum). During other periods, turn auto-registration off to prevent unauthorized devices from registering with Cisco Unified CallManager.	Enabling Autoregistration, *Cisco Unified CallManager Administration Guide* Disabling Autoregistration, *Cisco Unified CallManager Administration Guide*
Step 7	Install the devices that you want to autoregister.	Refer to the installation instructions that come with your IP phones and gateways.

Table 12-1 Autoregistration Configuration Checklist (continued)

Configuration Steps		Procedures and related topics
Step 8	Reconfigure the autoregistered devices and assign them to their permanent device pools.	Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide* Gateway Configuration, *Cisco Unified CallManager Administration Guide*
Step 9	In the Enterprise Parameters Configuration window, set the Auto Registration Phone Protocol setting to SIP or SCCP, whichever is needed. If auto registering more phones with a different protocol is required, repeat the preceding steps.	Enterprise Parameters Configuration, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topics

- System-Level Configuration Settings, page 5-1
- Redundancy, page 7-1
- SIP Line Side Overview, page 41-15
- Cisco Unified CallManager Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified CallManager Group Configuration, *Cisco Unified CallManager Administration Guide*
- Device Pool Configuration, *Cisco Unified CallManager Administration Guide*
- Enterprise Parameters Configuration, *Cisco Unified CallManager Administration Guide*

CHAPTER 13

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) server enables Cisco Unified IP Phones, connected to either the customer's data or voice Ethernet network, to dynamically obtain their IP addresses and configuration information. It uses Domain Name System (DNS) to resolve host names both within and outside the cluster. For information on configuring DHCP servers and subnets refer to "DHCP Server Configuration" in the *Cisco Unified CallManager Administration Guide*.

This section covers the following topics:

- DHCP Server, page 13-1
- Domain Name System, page 13-2
- Understanding How Devices Identify the TFTP Server, page 13-3
- Migration, page 13-4
- Alarms, page 13-4
- Related Topics, page 13-4

DHCP Server

Only one DHCP server per Cisco Unified CallManager cluster should exist. Different clusters can share one DHCP server, provided the Cisco Unified CallManager clusters are not geographically separated. In the later case, it may need one DHCP server per location. If the DHCP server is shared, some Cisco Unified CallManager clusters may have zero DHCP servers.

Because DHCP server is a standalone server, no backup server exists in case the Cisco Unified CallManager that is configured as DHCP server fails.

Cisco Unified CallManager administrator configures the DHCP servers and subnets. You can configure one server for each node and multiple subnets for each server.

Note You must update the DNS server with the appropriate Cisco Unified CallManager name and address information before using that information to configure the Cisco Unified CallManager server.

For Cisco Unified CallManager, you must reboot the node, if an IP address changes. As long as the node is up, it will keep refreshing the lease period for which the DHCP server provides an IP address, and hence retain the same IP address. However, hostname of the node must remain the same, even if the IP address changes.

Additional Information

See the "Related Topics" section on page 13-4.

Domain Name System

Two types of implementations exist for DNS.

- Corporate DNS, if available
- Internal DDNS service transparent to the user

The Cisco Unified CallManager administration provides support to configure different scopes for the DHCP server. For each scope, you can enter a range of IP addresses and subnet masks and you can also configure options.

For configuring DNS with Corporate DNS, the corporate DNS infrastructure is used, and default DNS configuration will act as a cache only service to this corporate DNS service.

When no corporate DNS service exists, Dynamic Domain Name System (DDNS) service, a service that allows dynamic updates to hostname and IP addresses, is used to implement a clusterwide DNS infrastructure. This also serves other devices on the network that are interacting with the cluster. Each node has DNS running on it. These DNS servers get configured with hostname and IP address information for all the nodes and any other devices in the cluster. The DNS on the first node in the cluster gets configured as primary DNS, while all other nodes get configured as secondary nodes.

When any change to DNS configuration occurs to the first node of Cisco Unified CallManager, it automatically gets transferred to other nodes. Other devices in the network can point to any of the nodes in the cluster for the DNS lookups.

Note Any change to the hostname of a node will require the node to be reinserted in the cluster.

When nodes are being configured using by DHCP, the DHCP client on the node will get configured to dynamically update DDNS.

Whenever nodes are configured by using DHCP, one the following events occurs:

- The corporate DNS can accept dynamic updates.
- DNS gets updated within the cluster
- DHCP configuration for the nodes gets tied with their MAC addresses of the node for which you are requesting an IP address. If the node requests an IP address again, DHCP matches the MAC address to the previous request and provides the same IP address.

You must update the DNS server with the appropriate Cisco Unified CallManager name and address information before using that information to configure the Cisco Unified CallManager server.

Additional Information

See the "Related Topics" section on page 13-4.

DHCP Server Configuration Process

Use the following steps to configure DHCP Process:

1. Enable the DHCP functionality from the serviceability window.
2. Verify the DHCP monitor process is started on the node where the DHCP is enabled.
3. Use Cisco Unified CallManager Administration to configure the scopes and options.
4. Verify that configuration is captured in the /etc/dhcpd.conf file of targeted Cisco Unified CallManager.
5. Verify the DHCP server daemon is running with new configuration.
6. Make sure DHCP monitor process logs at the specific trace settings.
7. Make sure the error alarm is raised when the DHCP daemon is stopped and the info alarm is raised when the daemon is restarted.

Additional Information

See the "Related Topics" section on page 13-4.

Understanding How Devices Identify the TFTP Server

The phones have an order of preference that they use for selecting the address of the TFTP (Trivial File Transfer Protocol) server. If the devices receive conflicting or confusing information from the DHCP server, the device uses the following sequence to determine what information is valid:

1. You can locally configure the phone with a TFTP server. This address overrides any TFTP address sent by the DHCP server. The phone always tries to resolve the DNS name CiscoCM1.
2. If this name is resolved, then it overrides all information sent by the DHCP server.

   It is not necessary to name the TFTP server CiscoCM1, but you must enter a DNS CName record to associate CiscoCM1 with the address or name of the TFTP server.
3. The phone uses the value of Next-Server in the boot processes. This DHCP configuration parameter has traditionally been used as the address of the TFTP server. When configuring BOOTP servers, this field is typically referred to as the address of the TFTP server.

   This information is returned in the siaddr field of the DHCP header. You should always use this option, if available, because some DHCP servers will place their own IP address in this field when it is not configured.
4. The phone uses the site-specific option 150.
5. The phone also accepts the Optional Server Name parameter. This DHCP configuration parameter is the DNS name of a TFTP server. Currently only a DNS name can be configured in this parameter; a dotted decimal IP address should not be used.
6. The phone also accepts the 66 option, which is the name of the boot server.
7. Option 66 is normally used to replace the sname field when option overloading occurs. It can be used on Windows NT DHCP servers and functions like the 150 option. This name field can contain a DNS name or a dotted decimal IP address.

8. The 66 option should not be used with the 150 option. If they are sent together, then the phone prefers the IP address over the name given by the 66 option. However, if both a dotted decimal IP address and a 150 option are sent, then order of preference is dependent on the order that they appear in the option list. The phone chooses the last item in the option list. To reiterate, option 66 and option 150 are mutually exclusive.

Additional Information

See the "Related Topics" section on page 13-4.

Migration

Because no migration is provided from Window 2000 based DHCP configuration to the DHCP configuration, the administrator needs to reconfigure the system.

Additional Information

See the "Related Topics" section on page 13-4.

Alarms

Two alarms are generated for DHCP.

- CiscoDhcpdFailure
- CiscoDhcpdRestarted

See the *Cisco Unified CallManager Serviceability Administration Guide* for more information on alarms.

Additional Information

See the "Related Topics" section on page 13-4.

Related Topics

- DHCP Server Configuration, *Cisco Unified CallManager Administration Guide*
- DHCP Subnet Configuration, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Security Guide*

Licensing

Implement licensing in Cisco Unified CallManager administration to accurately track the number of devices that a customer has connected to Cisco Unified CallManager, including third party SIP phones and compare it with the number of unit licenses that have been purchased.

Licensing feature helps in managing Cisco Unified CallManager licenses and in enforcing the licenses for Cisco Unified CallManager applications and the number of IP phones. Using the Licensing Configuration window in Cisco Unified CallManager Administration, you can manage the phone and node licenses purchased and used by the customer.

Licenses are generated for requested Cisco Unified CallManager nodes (servers in a Cisco Unified CallManager cluster) and the phones that are associated with those nodes.

Each phone type requires a fixed number of licenses and this number is called as phone license unit. For example, Cisco 7920 phones require four license units and Cisco 7970 phones require 5 units. If you want licenses for four Cisco 7920 phones and four Cisco 7970 phones, then you require 36 phone license units.

To determine the number of units of licenses required for each phone, see *Cisco Unified CallManager Administration Guide*.

This section covers the following topics:

- Starting License Manager Service, page 14-1
- Splitting Licenses, page 14-2
- Alarms, page 14-3
- Migrating from Cisco Unified CallManager 4.0(x) to 5.0(x), page 14-3
- Transferring License Files, page 14-4
- Related Topics, page 14-4

Starting License Manager Service

The Cisco Unified CallManager server where the license file is loaded, assumes the functionality of a license manager. For information on license files refer to *Cisco Unified CallManager Administration Guide*.

The license manager serves as the logical component that keeps track of the licenses that the customer purchases and the licenses that customer uses. It refers to the processes that control the checkin and checkout of the licenses. It keeps track of the number of license units that are required for each phone type. The license manager has responsibility for issuing and reclaiming licenses, and detecting whether there is an overdraft of licenses.

Start license manager service using Cisco Unified CallManager Serviceability. This section describes the procedures to start, stop, or restart the service.

Procedure

Step 1 In Cisco Unified CallManager Serviceability, choose **Tools > Control Center - Network Services.**

The Control Center–Network Services window displays.

Step 2 Choose the Cisco Unified CallManager server from the Servers drop-down list box.

Cisco License Manager displays in list under Service Name column, in the Platform Services.

Step 3 Click the radio button corresponding to Cisco License Manager.

Step 4 If you want to start License Manager service, click **Start**.

The service starts, and the message, Service Started Successfully, displays.

Step 5 If you want to stop the License Manager service, click **Stop**.

The service stops, and the message, Service Successfully Stopped, displays.

Step 6 If you want to restart the License Manager, click **Restart**.

The service restarts, and the message, Service Successfully Restarted, displays.

Additional Information

See the "Related Topics" section on page 14-4.

Splitting Licenses

When you place an order for Cisco devices, Cisco provides a Product Authorization Key (PAK).Using PAK, you can split the licenses across multiple clusters.

Note Cisco Product Marketing team will determine whether splitting of licenses across clusters is allowed for a PAK, depending on the number of licenses that are purchased.

For example, you request 20 Cisco Unified CallManager nodes and 20000 phone units in one purchase order. A PAK gets issued once the request is approved. Using this PAK, you can split the licenses across multiple clusters with one license file containing 15 Cisco Unified CallManager nodes and 15000 phone units, and another license file with 5 Cisco Unified CallManager nodes and 5000 phone units.

To determine the number of license unit that are required for each device, in Cisco Unified CallManager Administration, choose **System > Licensing > License Unit Calculator**. This window lists the number of license units that are required for each type of device.

Additional Information

See the "Related Topics" section on page 14-4.

Alarms

The following alarms are generated for licensing.

- CiscoLicenseManagerDown
- CiscoLicenseOverDraft
- CiscoLicenseRequestFailed
- CiscoLicenseDataStoreError
- CiscoLicenseInternalError
- CiscoLicenseFileError

See the *Cisco Unified CallManager Serviceability Administration Guide* for more information on alarms.

Additional Information

See the "Related Topics" section on page 14-4.

Migrating from Cisco Unified CallManager 4.0(x) to 5.0(x)

When you migrate from Cisco Unified CallManager version 4.0(x) to 5.0(x), the licenses that are required for existing phones and existing Cisco Unified CallManager nodes is calculated and an intermediate file (XML file) that contains these license counts will be generated during the Cisco Unified CallManager migration process. These licenses are given free of cost because you are already using these phones for Cisco Unified CallManager version 4.x. If you are provisioning new phones and nodes after migrating to Cisco Unified CallManager 5.0(x), you need to paste the intermediate license file in the License Registration window on CCO.

Use the following procedure to register existing licenses and request for new licenses.

Step 1 In Cisco Unified CallManager Administration, choose **System > Licensing > License File Upload**.

The License File Upload window displays.

Step 2 Click **View File**. A pop-up window displays that has the license information for existing phones and nodes. Copy this information. To copy the contents on this windrow, you can use **Ctrl-A** (Select All) and **Ctrl-C** (Copy).

Step 3 On the License Registration window of CCO website, in the text box provided, paste the file contents using **Ctrl-V**.

Step 4 You must enter the MAC address of the Cisco Unified CallManager server that you are requesting the licenses for, and a valid E-mail Id.

Step 5 To obtain the actual license file, click **Submit**. A license file is generated.

Step 6 You must upload the license file to the server with the matching MAC address that you provided in Step 4. See the "Uploading a License file" section in the *Cisco Unified CallManager Administration Guide*. This node takes on the functionality of the license manager.

Additional Information

See the "Related Topics" section on page 14-4.

Transferring License Files

When the first node fails on the Cisco Unified CallManager and a new node is configured as the first node, the license files need to be transferred to the new node.

Two scenarios might occur:

Scenario 1

The customer has already obtained the license file, but has not yet uploaded it to the license manager.

Solution Generate a new license file with the same license information but with a new MAC address.

Scenario 2

The customer has obtained the license file and uploaded the file to the license manager. The license information exits on the new node, but not the license file.

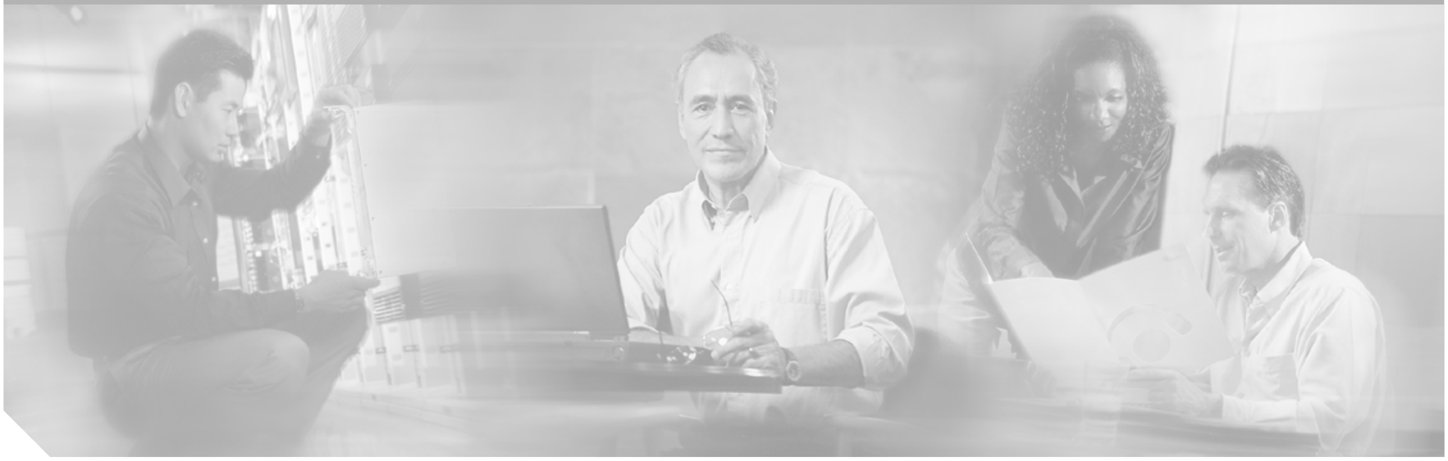
Solution Generate a new license file with the same license information but with a new MAC address.

Additional Information

See the "Related Topics" section on page 14-4.

Related Topics

- License File Upload, *Cisco Unified CallManager Administration Guide*
- License Unit Calculator, *Cisco Unified CallManager Administration Guide*
- License Unit Report, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Security Guide*
- *Cisco Unified CallManager Assistant User Guide*
- *Cisco IP Communicator Administration Guide*



PART 3

Dial Plan Architecture

CHAPTER 15

Partitions and Calling Search Spaces

Partitions and calling search spaces provide the capability for implementing calling restrictions and creating closed dial plan groups on the same Cisco Unified CallManager.

This section covers the following topics:

- Understanding Partitions and Calling Search Spaces, page 15-1
- Examples, page 15-2
- Guidelines and Tips, page 15-3
- Dependency Records, page 15-3
- Partition Name Limitations, page 15-4
- Where to Find More Information, page 15-4

Understanding Partitions and Calling Search Spaces

A partition comprises a logical grouping of directory numbers (DNs) and route patterns with similar reachability characteristics. Devices that are typically placed in partitions include DNs and route patterns. These entities associate with DNs that users dial. For simplicity, partition names usually reflect their characteristics, such as “NYLongDistancePT,” “NY911PT,” and so on.

A calling search space comprises an ordered list of partitions that users can look at before users are allowed to place a call. Calling search spaces determine the partitions that calling devices, including IP phones, softphones, and gateways, can search when attempting to complete a call.

When a calling search space is assigned to a device, the list of partitions in the calling search space comprises only the partitions that the device is allowed to reach. All other DNs that are in partitions not in the device calling search space receive a busy signal.

Partitions and calling search spaces address three specific problems:

- Routing by geographical location
- Routing by tenant
- Routing by class of user

Partitions and calling search spaces provide a way to segregate the global dialable address space. The global dialable address space comprises the complete set of dialing patterns to which Cisco Unified CallManager can respond.

Partitions do not significantly impact the performance of digit analysis, but every partition that is specified in a calling device search space does require that an additional analysis pass through the analysis data structures. The digit analysis process looks through every partition in a calling search space for the best match. The order of the partitions that are listed in the calling search space serves only to break ties when equally good matches occur in two different partitions. If no partition is specified for a pattern, the pattern goes in the null partition to resolve dialed digits. Digit analysis always looks through the null partition last.

You can associate partitions with a time schedule and a time zone. Associating a partition to a time schedule and a time zone allows configuration of time-of-day routing for calls that are coming into a partition and the partition's associated calling search spaces. Refer to "Time-of-Day Routing" for more information.

If you configure a calling search space both on an IP phone line and on the device (IP phone) itself, Cisco Unified CallManager concatenates the two calling search spaces and places the line calling search space in front of the device calling search space. If the same route pattern appears in two partitions, one contained in the line calling search space and one contained in the device calling search space, then Cisco Unified CallManager selects the route pattern that is listed first in the concatenated list of partitions (in this case, the route pattern that is associated with the line calling search space).

Note Cisco recommends avoiding the configuration of equally matching patterns in partitions that are part of the same calling search space or part of different calling search spaces that are configured on the same phone. This practice avoids the difficulties related to predicting dial plan routing when the calling search space partition order is used as a tie breaker.

Before you configure any partitions or calling search spaces, all directory numbers (DN) reside in a special partition named <None>, and all devices are assigned a calling search space also named <None>. When you create custom partitions and calling search spaces, any calling search space that you create also contains the <None> partition, while the <None> calling search space contains only the <None> partition.

Note Any device making a call can explicitly reach any dial plan entry that is left in the <None> partition. To avoid unexpected results, Cisco recommends that you do not leave dial plan entries in the <None> partition.

Examples

Calling search spaces determine partitions that calling devices search when they are attempting to complete a call.

For example, assume a calling search space named "Executive" includes four partitions: NYLongDistance, NYInternational, NYLocalCall, and NY911. Assume that another calling search space named "Guest" includes two partitions, NY911 and NYLocalCall.

If the Cisco IP Phone that is associated with a phone or line is in the "Executive" calling search space, the search looks at partitions "NYLongDistance," "NYInternationalCall," "NYLocalCall," and "NY911" when it attempts to initiate the call. Users who are calling from this number can place international calls, long-distance calls, local calls, and calls to 911.

If the Cisco Unified IP Phone that is associated with a phone or line is in the “Guest” calling search space, the search looks only at the “NYLocalCall” and “NY911” partitions when it initiates the call. If a user who is calling from this number tries to dial an international number, a match does not occur, and the call cannot be routed.

Guidelines and Tips

Use the following tips and guidelines when setting up partitions and calling search spaces:

- Use concise and descriptive names for your partitions. The CompanynameLocationCalltypePT format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a partition. For example, CiscoDallasMetroPT identifies a partition for toll-free inter-LATA (local access and transport area) calls from the Cisco office in Dallas.

  For more information about partition names and how they affect the number of partitions that are allowed, see the “Partition Name Limitations” section on page 15-4.
- To ensure that dialing privileges are uniform for all lines on a given phone, you may configure the calling search space on the IP phone itself and not on the individual lines of the phone. This practice prevents users from choosing another line on the phone to bypass calling restrictions.
- When configuring call forward features on an IP phone line, do not choose a calling search space that can reach the PSTN. This practice prevents users from forwarding their IP phone lines to a long-distance number and dialing their local IP phone number to bypass long-distance toll charges.

Dependency Records

If you need to find specific information about partitions and calling search spaces, click the Dependency Records link that is provided on the Cisco Unified CallManager Administration Partition Configuration and Calling Search Space Configuration windows. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Partition Dependency Records

The Dependency Records Summary window for partitions displays information about calling search spaces, route patterns, and directory numbers that are using the partition. To find more information, click the record type, and the Dependency Records Details window displays.

Calling Search Space

The Dependency Records Summary window for calling search spaces displays information about phones, gateways, voice-mail ports, and device pools that are using the calling search space. To find more information, click the record type, and the Dependency Records Details window displays.

For more information about Dependency Records, refer to Accessing Dependency Records in the *Cisco Unified CallManager Administration Guide*.

Partition Name Limitations

A calling search space (CSS) clause that call processing uses internally limits the maximum number of partitions. The CSS clause comprises the list of partitions in the calling search space by name. The CSS clause that call processing uses comprises a combination of a device CSS and the CSS for the directory number (DN) or route pattern that is associated with the device (for example, a line on a phone).

The maximum length of the combined CSS clause (device and pattern) comprises 1024 characters, including separator characters between partition names (for example, "partition 1:partition 2:partition 3"). Because the CSS clause uses partition names, the maximum number of partitions in a CSS varies depending on the length of the partition names. Also, because the CSS clause combines the CSS of the device and the CSS of the route pattern, the maximum character limit for an individual CSS specifies 512 (half of the combined CSS clause limit of 1024 characters).

When you are creating partitions and calling search spaces, keep the names of partitions short relative to the number of partitions that you plan to include in a calling search space. Refer to "Calling Search Space Configuration Settings" in the *Cisco Unified CallManager Administration Guide* for examples of the maximum number of partitions that can be added to a calling search space if the partition names are of fixed length.

Where to Find More Information

Related Topics

- Understanding Route Plans, page 17-1

Additional Cisco Documentation

- Calling Search Space Configuration, *Cisco Unified CallManager Administration Guide*
- Partition Configuration, *Cisco Unified CallManager Administration Guide*
- Calling Search Space Configuration, *Cisco Unified CallManager Administration Guide*
- Time-of-Day Routing, page 16-1
- Time Period Configuration, *Cisco Unified CallManager Administration Guide*
- Time Schedule Configuration, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design*

Time-of-Day Routing

Time-of-Day routing routes calls to different locations based on the time of day when a call is made. For example, during business hours, calls can route to an office, and after hours, calls can go directly to a voice-messaging system or to a home number.

This section covers the following topics:

- Understanding Time-of-Day Routing, page 16-1
- End-Users and Time-of-Day Routing, page 16-2
- Dependency Records, page 16-3
- Where to Find More Information, page 16-3

Understanding Time-of-Day Routing

Time-of-Day routing comprises individual time periods that the administrator defines and groups into time schedules. The administrator associates time schedules with a partition. In the Partition Configuration window, the administrator chooses either the time zone of the originating device or any specific time zone for a time schedule. The system checks the chosen time zone against the time schedule when the call gets placed to directory numbers in this partition. The Time Period and Time Schedule menu items exist in the Route Plan menu under the Class of Control submenu. The Partition and Calling Search Space menu items also have moved to the Class of Control submenu.

Time Periods

A time period comprises a start time and end time. The available start times and end times comprise 15-minute intervals on a 24-hour clock from 00:00 to 24:00. Additionally, a time period requires definition of a repetition interval. Repetition intervals comprise the days of the week (for example, Monday through Friday) or a day of the calendar year (for example, June 9).

Examples

You can define time period *weekdayofficehours* as 08:00 to 17:00 from Monday to Friday.

You can define time period *newyearsday* as 00:00 to 24:00 on January 1.

You can define time period *noofficehours* that has no office hours on Wednesdays. For this time period, the associated partition is not active on Wednesdays.

Note In defining a time period, the start time must precede (be less than) the end time.

Tip To define an overnight time span that starts on Monday through Friday at 22:00 and ends at 04:00 the next morning, create two time periods, such as *lateevening* (from 22:00 to 24:00 on Monday through Friday) and *earlymorning* (from 00:00 to 04:00 on Tuesday through Saturday). Use the Time Schedule Configuration window to associate the *lateevening* and *earlymorning* time periods into a single time schedule that spans the overnight hours.

After the administrator creates a time period, the administrator must associate the time period with a time schedule.

Time Schedules

A time schedule comprises a group of defined time periods that the administrator associates. After the administrator has configured a time period, the time period displays in the Available Time Periods list box in the Time Schedule Configuration window. The administrator can select a time period and add it to the Selected Time Periods list box.

Note After the administrator selects a time period for association with a time schedule, the time period remains available for association with other time schedules.

After the administrator has configured a time schedule, the administrator can use the Partition Configuration window to select either the time zone of the originating device or any specific time zone for a defined time schedule. The selected time zone gets checked against the time schedule when the user places the call.

The Time-of-Day feature filters the CallingSearchSpace string through Time-of-day settings that are defined for each partition in the CallingSearchSpace.

After time-of-day routing is configured, if the time of an incoming call is within one of the time periods in the time schedule, the partition gets included in the filtered partition list search for the call.

Examples

You can define time schedule *USAholidays* as the group of the following time periods: newyearsday, presidentsday, memorialday, independenceday, laborday, thanksgivingday, christmasday. The administrator must first configure the applicable time periods.

You can define time schedule *library_open_hours* as the group of the following time periods: Mon_to_Fri_hours, Sat_hours, Sun_hours. The administrator must first configure the applicable time periods.

End-Users and Time-of-Day Routing

If time-of-day routing is enforced, users cannot set certain CFwdAll numbers at certain times. For example, User A’s Calling Search Space for forwarding includes a Time-of-Day-configured partition that allows international calls from 08:00 to 17:00 (5:00 pm). User A wants to configure his CFwdAll number to an international number. He can only set this number during the 08:00-to-17:00 time period because, outside these hours, the system does not find the international number in the partition that is used to validate the CFwdAll number.

If the user sets the CFwdAll during office hours when it is allowed, and the user receives a call outside office hours, the caller hears fast-busy.

Users cannot reach directory numbers in some partitions that are configured for time-of-day routing and that are not active during the time of call, depending upon the configuration of partitions.

Users also cannot reach the Route/Translation pattern in partitions configured with time-of-day routing which is not active at the time of call.

Note Although a user may not be able to set Forward All for a phone due to the partition and time-of-day settings that apply to the phone, an administrator or a user can still set the Call Forward All option on the phone from the Cisco Unified CallManager Administration page.

Note TOD settings comes into effect when the lines are included in a Hunt List. The settings only apply to the Hunt Pilot and not to the lines within that Hunt List.

Dependency Records

If you need to find specific information about time periods and time schedules, click the Dependency Records link that is provided on the Cisco Unified CallManager Administration Time Period Configuration and Time Schedule Configuration windows. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Time Period Dependency Records

The Dependency Records Summary window for time periods displays information about time schedules that are using the time period. To find more information, click the record type, and the Dependency Records Details window displays.

Time Schedule Dependency Records

The Dependency Records Summary window for time schedules displays information about partitions that are using the time schedule. To find more information, click the record type, and the Dependency Records Details window displays.

For more information about Dependency Records, refer to Accessing Dependency Records, *Cisco Unified CallManager Administration Guide*.

Where to Find More Information

Related Topics

- Time Period Configuration, *Cisco Unified CallManager Administration Guide*
- Time Schedule Configuration, *Cisco Unified CallManager Administration Guide*
- Partition Configuration, *Cisco Unified CallManager Administration Guide*
- Calling Search Space Configuration, *Cisco Unified CallManager Administration Guide*

- Partitions and Calling Search Spaces, page 15-1
- Understanding Route Plans, page 17-1

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design*

CHAPTER 17

Understanding Route Plans

The Route Plan drop-down list on the menu bar allows you to configure Cisco Unified CallManager route plans by using route patterns, route filters, route lists, and route groups, as well as hunt pilots, hunt lists, and line groups.

This section describes the following route plan topics:

- Automated Alternate Routing, page 17-1
- Route Plan Overview, page 17-4
- Route Groups and Route Lists, page 17-5
- Route Patterns, page 17-6
- Hunt Lists, page 17-9
- Hunt Pilots, page 17-9
- Call Coverage, page 17-10
- Closest Match Routing, page 17-12
- Static Digit Analysis, page 17-13
- Special Characters and Settings, page 17-15
- Calling and Called Party Transformations, page 17-25
- Caller Identification and Restriction, page 17-28
- External Route Plan Wizard, page 17-33
- Route Plan Report, page 17-37
- Where to Find More Information, page 17-37

Automated Alternate Routing

Automated alternate routing (AAR) provides a mechanism to reroute calls through the PSTN or other network by using an alternate number. As a subset of the AAR feature, Cisco Unified CallManager automatically reroutes calls through the PSTN or other networks when Cisco Unified CallManager blocks a call due to insufficient location bandwidth. With automated alternate routing, the caller does not need to hang up and redial the called party.

When a call is made from the device of one location to the device of another location, location bandwidth gets deducted from the maximum available bandwidth that is available for the call at either location. If not enough location bandwidth for the call exists at either location, instead of blocking the call, Cisco Unified CallManager uses the table of AAR groups and the external number of the terminating directory number to supply the alternate number that is used to reroute the call through the PSTN or other network. The Cisco Unified IP Phone displays the message “Network congestion, rerouting.” (Configure this message by using Service Parameters Configuration for the Cisco CallManager service.) Cisco Unified CallManager automatically attempts to reroute the call by using the alternate number. If the reroute is successful, the caller connects to the called party.

AAR supports the following call scenarios for insufficient bandwidth:

- Call originates from a line or directory number (DN) of an IP phone within one location and terminates to a line or DN of another IP phone within another location. This scenario includes calls that terminate at the shared line with terminating IP phone devices that are resident in multiple locations and calls that terminate at the Cisco voice-mail port.
- Incoming call through a gateway device within one location terminates to a line or DN of an IP phone within another location. This scenario includes calls that terminate at the shared line with terminating IP phone devices that are resident in multiple locations and calls that terminate at the Cisco voice-mail port.

Cisco Unified CallManager automatically attempts to reroute calls, due to insufficient bandwidth, through the PSTN or other network only when the AAREnable enterprise parameter is set to true. Cisco Unified CallManager uses the device-based AAR calling search space, which is assigned to Cisco Unified IP Phone station devices and gateway devices, when it attempts to route the call to the gateway device that connects to the PSTN or other network. Cisco Unified CallManager uses the external phone number mask and the directory number of the line or DN and the Cisco voice-mail port to derive the alternate number that is used to reroute the call.

Automated Alternate Routing Example

In the following scenario, line/DN 5000 in the Richardson AAR group calls line 5001 in the San Jose AAR group. If not enough location bandwidth exists, the call attempts to reroute through the PSTN or other network. To route the call from AAR group Richardson to AAR group San Jose, Cisco Unified CallManager needs to know the access digit(s) to dial out to the PSTN or other network, the long-distance dialing requirement, if any, and the alternate number. Cisco Unified CallManager retrieves the information from the AAR dial prefix matrix table, which is indexed by the originating line AAR group value and the terminating line AAR group value. Table 17-1 shows how the AAR group field is data filled in the line/DN table:

Table 17-1 Line/DN and AAR Group Association

Line/DN	AAR Group
5000	Richardson
5001	San Jose
5002	Dallas

Cisco Unified CallManager retrieves the prefix digits from the AAR dial prefix matrix table based on the AAR group value of the originating line/DN and gateway device and the AAR group value of the terminating line, and Cisco voice-mail port, to transform the derived alternate number. Table 17-2 shows an example of how the AAR dial prefix matrix table is data filled:

Table 17-2 AAR Dial Prefix Matrix Table Example

From AAR Group	To AAR Group	Prefix Digits
Richardson	San Jose	91
Richardson	Dallas	9
Richardson	Richardson	9
San Jose	Richardson	91
San Jose	Dallas	91
San Jose	San Jose	9
Dallas	Richardson	9
Dallas	San Jose	91
Dallas	Dallas	9

Cisco Unified CallManager prepends the prefix digits that are retrieved from the AAR dial prefix matrix table to the derived alternate number. Digit analysis uses the transformed digits, plus the AAR calling search space, to route the call to the PSTN or other network.

A much greater rate of success for automated alternate routing occurs when a gateway is located in the same location as the originating or terminating device. Therefore, a call that is outgoing to the PSTN or other network from a gateway that is located in the same location as the originating device and that is also incoming from a gateway located in the same location as the terminating device describes the best scenario. In other scenarios, the call remains subject to location bandwidth validation between the originating device and outgoing gateway, and between the terminating device and incoming gateway.

Automated Alternate Routing Enable Service Parameter

Besides configuring AAR groups, ensure that the Automated Alternate Routing Enable clusterwide service parameter is set to *True*. (The default value for this service parameter specifies *False*.)

The Clusterwide Parameters (System - CCMAutomated Alternate Routing) section of the service parameters for the Cisco CallManager service includes the parameter.

Automated Alternate Routing and Hunt Pilots

In previous Cisco Unified CallManager releases, if the voice messaging system is in a central location and the user is in a remote location, when the remote user tries to reach the voice messaging system and bandwidth is not available on the WAN link, Cisco Unified CallManager can reroute the call through the PSTN to the voice messaging system.

In the current Cisco Unified CallManager release, AAR does not automatically work with hunt pilots. Because the fully qualified directory number (DN) of the remote agent is unknown, AAR cannot initiate the reroute.

To enable AAR to work with hunt pilots, two additional fields display in the Hunt Pilot Configuration window: AAR Group and External Number Mask. For each hunt pilot, you must configure these fields in the Hunt Pilot Configuration window for AAR groups to work with hunt pilots. Refer to the "Hunt Pilot Configuration" chapter in the *Cisco Unified CallManager Administration Guide* for details.

Route Plan Overview

Cisco Unified CallManager uses route plans to route internal calls within a Cisco Unified CallManager cluster, and external calls to a private network or the public switched telephone network (PSTN).

Route patterns, route filters, route lists, route groups, line groups, hunt lists, and hunt pilots provide flexibility in network design. Route patterns work in conjunction with route filters to direct calls to specific devices and to include or exclude specific digit patterns. Use route patterns to include and exclude digit patterns. Use route filters primarily to include digit patterns. Route lists control the selection order of the route groups. Route groups set the selection order of the gateway devices.

You can assign route patterns to gateways, to trunks, or to a route list that contains one or more route groups. Route groups determine the order of preference for gateway and trunk usage. Route groups allow overflows from busy or failed devices to alternate devices.

Route lists determine the order of preference for route group usage. If a route list is configured, you must configure at least one route group. One or more route lists can point to one or more route groups.

Route filters may restrict certain numbers that are otherwise allowed by a route pattern from being routed. Tags, or clauses, provide the core component of route filters. A tag applies a name to a portion of the dialed digits. For example, the North American Numbering Plan (NANP) number 972-555-1234 contains the LOCAL-AREA-CODE (972), OFFICE-CODE (555), and SUBSCRIBER (1234) tags.

Note The NANP designates the numbering plan for the PSTN in the United States and its territories, Canada, Bermuda, and many Caribbean nations. NANP includes any number that can be dialed and is recognized in North America.

Route patterns represent all valid digit strings. Cisco Analog Access Trunk Gateways, Cisco Digital Access Trunk Gateways, Cisco MGCP gateways, H.323-compliant gateways, and trunks also use route patterns. Cisco gateways can route ranges of numbers with complex restrictions and manipulate directory numbers before the Cisco Unified CallManager passes them on to an adjacent system. The adjacent system can include a central office (CO), a private branch exchange (PBX), or a gateway on another Cisco Unified CallManager system.

Line groups consists of list of DNs. Line groups specify a distribution algorithm (such as Top Down) for the members of the line group. Line groups also specify the hunt options to use in cases where the line group members do not answer, are busy, or are not available. Beginning with Release 4.1 of Cisco Unified CallManager, a directory number may belong to more than one line group.

Hunt lists comprise ordered groupings of line groups. A line group may belong to more than one hunt list. A hunt list must specify at least one line group before the hunt list can accept calls.

Hunt pilots represent route patterns that are used for hunting. A hunt pilot can specify a partition, numbering plan, route filter, and hunt forward settings. A hunt pilot must specify a hunt list.

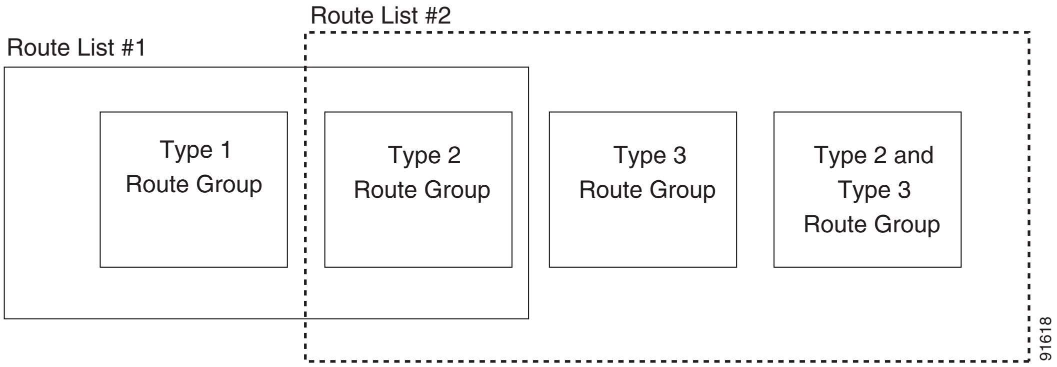
Route Groups and Route Lists

Route groups contain one or more devices, and route lists contain one or more route groups. Cisco Unified CallManager may restrict the gateways that you can include in the same route group and the route groups that you can include in the same route list. For the purpose of route group and route list restrictions, Cisco Unified CallManager divides gateways into three types:

- Type 1—MGCP QSIG gateways and QSIG-enabled intercluster trunks
- Type 2—MGCP non-QSIG, Skinny, T1-CAS gateways; non-QSIG intercluster trunks
- Type 3—H.225 and H.323 gateways, and all other trunk types

Route lists can contain a mixture of route group types, although you cannot combine an H225 trunk with a Type 1 (QSIG) route group. Cisco Unified CallManager does not allow you to add route groups that contain gateways that use the H.323 or H.225 protocol (Type 3) and route groups that contain MGCP gateways that use a QSIG protocol (Type 1) to the same route list. You can create route lists with any combination of Type 1 route groups and Type 2 route groups as well as with any combination of Type 2 route groups and Type 3 route groups, as illustrated in Figure 17-1.

Figure 17-1 Valid Route Lists Example



For more information on creating route groups, refer to the "Configuring a Route Group" section in the *Cisco Unified CallManager Administration Guide*. For more information on creating route lists, refer to the "Adding a Route List" section in the *Cisco Unified CallManager Administration Guide*.

Note As of Release 4.1 of Cisco Unified CallManager, you cannot combine route groups and line groups, and route lists and hunt lists become separate entities. Thus, route groups make up route lists, and line groups make up hunt lists. In Release 4.0 of Cisco Unified CallManager, possible components of route/hunt lists included both route groups and line groups.

Note In Release 4.0 of Cisco Unified CallManager, possible members of route/hunt lists included both line groups and route groups. In Release 4.1 of Cisco Unified CallManager, if an existing route/hunt list includes a line group as a member, Cisco Unified CallManager migrates the route/hunt list to a hunt list.

Route Patterns

Cisco Unified CallManager uses route patterns to route or block both internal and external calls.

Note Prior to Release 4.1 of Cisco Unified CallManager, configuration of route patterns and hunt pilots occurred in a single window, since Route Pattern and Hunt Pilot were integrated. Route List and Hunt list were part of the same list. A list could have a Line Group and/or Route Groups.

Note Starting with Release 4.1, Route Group and Route lists are part of Route Pattern configuration. Line groups and Hunt lists are part of Hunt pilot configuration. Route Patterns and Hunt Pilots are configured separately. Route Groups or Route Lists cannot be added to Hunt Pilot and Line Groups. Hunt Lists cannot be added to Route Pattern. If an existing route pattern/hunt pilot associates with a hunt list, Cisco Unified CallManager migrates the route pattern/hunt pilot to a hunt pilot.

The simplest route pattern specifies a set of one or more digits. For example, the number 8912 specifies a route pattern.

Gateways and Cisco Unified IP Phones can also use more complex route patterns that can contain wildcards. A wildcard represents a range of numbers; for example, X represents any digit 0 through 9.

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.

Caution If a gateway has no route pattern that is associated with it, or it does not belong to a route group, it cannot route any calls.

You can use route patterns to invoke network-specific services/facilities on a call-by-call basis by configuring the fields in the ISDN Network-Specific Facilities Information Element section on the Route Pattern Configuration window. Cisco Unified CallManager uses the network-specific services/facilities when the user dials the route pattern.

Note Cisco Unified CallManager only uses the network-specific information with PRI protocol gateways. H.323 gateways do not support network-specific facilities, but they support SDN when the dial peers are configured accordingly. Cisco Unified CallManager codes the bearer capability as Speech for the ACCUNET service.

Route Pattern Usage

You can assign a route pattern directly to a Cisco Access Gateway, or you can assign it to a route list for more flexibility. For example, Figure 17-2 shows Cisco Digital Access Gateway 1 designated as the first choice for routing outgoing calls to the PSTN when a matching route pattern is dialed.

Tip If a gateway does not have a route pattern, it cannot place calls to the PSTN or to a PBX. To assign a route pattern to an individual port on a gateway, you must assign a route list and a route group to that port.

Figure 17-2 shows the effects of using route patterns with Cisco Digital Gateways. This example assigns the route pattern to a route list, and that route list associates with a single route group. The route group supports a list of devices that are selected based on availability. If all ports on the first-choice gateway are busy or out of service, the call routes to the second-choice gateway in the route group.

Note If a route pattern is associated with a gateway, and all the resources of that gateway are used, then the call does not get routed.

Figure 17-2 Route Plan Summary Diagram for Cisco Digital Gateways

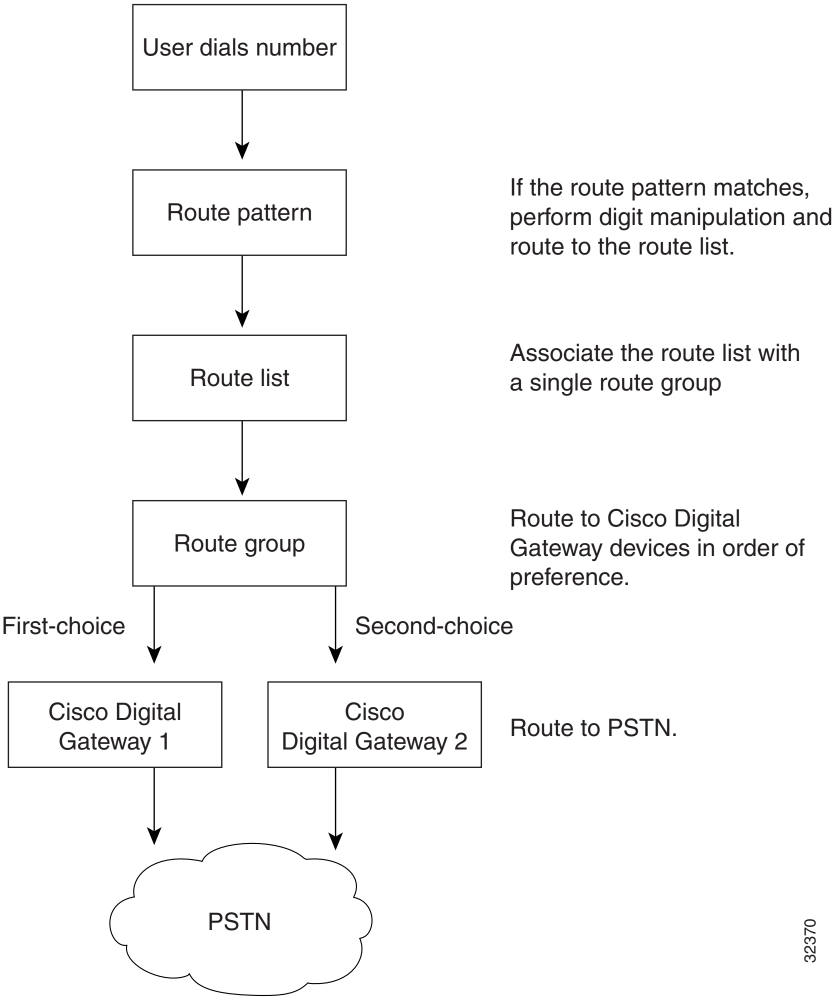
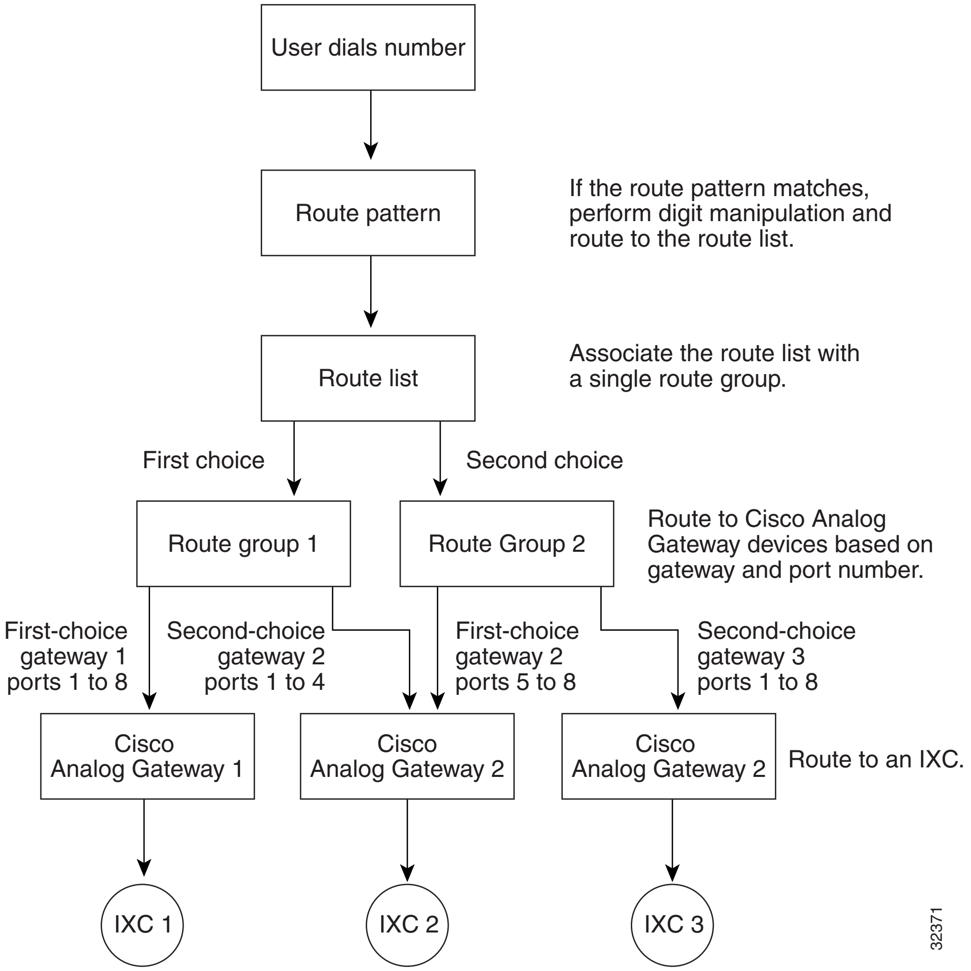

User dials number
Route pattern
If the route pattern matches, perform digit manipulation and route to the route list.
Route list
Associate the route list with a single route group
Route group
Route to Cisco Digital Gateway devices in order of preference.
First-choice
Second-choice
Cisco Digital Gateway 1
Cisco Digital Gateway 2
Route to PSTN.
PSTN
32370

Figure 17-3 shows the effects of using route patterns with Cisco Analog Gateways. This example assigns the route pattern to a route list, and that route list associates with two route groups. Route group 1 associates with ports 1 through 8 on gateway 1, which routes all calls to interexchange carrier 1 (IXC 1). Route group 1 also associates with ports 1 through 4 on gateway 2. Route group 2 associates with ports 5 through 8 on gateway 2 and all ports on gateway 3.

Each route group supports a list of devices that are chosen on the basis of availability. For route group 1, if ports 1 through 8 on the first-choice gateway are busy or out of service, calls route to ports 1 through 4 on the second-choice gateway. If all routes in route group 1 are unavailable, calls route to route group 2. For route group 2, if ports 5 through 8 on the first-choice gateway are busy or out of service, calls route to ports 1 through 8 on the second-choice gateway. If no ports on any gateway in either route group are available, the call routes to an all trunks busy tone.

Figure 17-3 Route Plan Summary Diagram for Cisco Analog Access Gateways


User dials number
Route pattern
If the route pattern matches, perform digit manipulation and route to the route list.
Route list
Associate the route list with a single route group.
First choice
Second choice
Route group 1
Route Group 2
Route to Cisco Analog Gateway devices based on gateway and port number.
First-choice gateway 1 ports 1 to 8
Second-choice gateway 2 ports 1 to 4
First-choice gateway 2 ports 5 to 8
Second-choice gateway 3 ports 1 to 8
Cisco Analog Gateway 1
Cisco Analog Gateway 2
Cisco Analog Gateway 2
Route to an IXC.
IXC 1
IXC 2
IXC 3
32371

Line Groups

Line groups contain one or more directory numbers. A distribution algorithm, such as Top Down, Circular, Longest Idle Time, or Broadcast, associates with a line group. Line groups also have an associated Ring No Answer reversion timeout value.

The following descriptions apply to the members of a line group:

- An *idle* member designates one that is not serving any call.
- An *available* member designates one that is serving an active call but can accept a new call(s).
- A *busy* member cannot accept any calls.

For information on configuring line groups, refer to the "Line Group Configuration" section in the *Cisco Unified CallManager Administration Guide*.

Note Prior to Release 4.1 of Cisco Unified CallManager, line groups could belong to route/hunt lists. Beginning with Release 4.1 of Cisco Unified CallManager, line groups belong to hunt lists, whereas route groups belong to route lists.

Beginning with Release 4.1 of Cisco Unified CallManager, a directory number may belong to more than one line group.

Hunt Lists

Hunt lists comprise ordered groupings of line groups. A line group may belong to more than one hunt list. Hunt pilots associate with hunt lists. A hunt list may associate with more than one hunt pilot.

For information on configuring hunt lists, refer to the "Hunt List Configuration" section in the *Cisco Unified CallManager Administration Guide*.

Note Prior to Release 4.1 of Cisco Unified CallManager, configuration of hunt lists and route lists occurred in a single window. Starting with Release 4.1, configuration of hunt lists and route lists occurs separately.

Note In Release 4.0 of Cisco Unified CallManager, both line groups and route groups represent possible members of route/hunt lists. In Release 4.1 of Cisco Unified CallManager, if an existing route/hunt list has a line group as a member, Cisco Unified CallManager migrates the route/hunt list to a hunt list.

Note TOD settings comes into effect when the lines are included in a Hunt List. The settings only apply to the Hunt Pilot and not to the lines within that Hunt List.

Hunt Pilots

Hunt pilots are sets of digits. They comprise lists of route patterns that are used for hunting. A hunt pilot can specify a partition, numbering plan, route filter, and hunt forward settings. A hunt pilot must specify a hunt list.

For information on configuring hunt pilots, refer to the "Hunt Pilot Configuration" section in the *Cisco Unified CallManager Administration Guide*.

Note Prior to Release 4.1 of Cisco Unified CallManager, configuration of hunt pilots and route patterns occurred in a single window. Starting with Release 4.1, configuration of hunt pilots and route patterns occurs separately.

Note In Release 4.0 of Cisco Unified CallManager, both route lists and hunt lists associated with route patterns/hunt pilots. In Release 4.1 of Cisco Unified CallManager, if an existing route pattern/hunt pilot associates with a hunt list, Cisco Unified CallManager migrates the route pattern/hunt pilot to a hunt pilot.

Note TOD settings comes into effect when the lines are included in a Hunt List. The settings only apply to the Hunt Pilot and not to the lines within that Hunt List.

Call Coverage

The Call Coverage feature, implemented first in Release 4.1 of Cisco Unified CallManager, comprises the following Cisco Unified CallManager capabilities:

- Forwarding provides separate configuration based on whether the call originator is an internal user or an external user. Refer to the "Internal and External Calls" section on page 17-11.
- Hunting supports personal forwarding. Refer to the "Personal Preferences" section on page 17-11.
- In Cisco Unified CallManager 4.0, route patterns and hunt pilots are in one feature. In Cisco Unified CallManager 4.1 and subsequent releases, they are separated in two different features.

Hunting and Call Forwarding

The concept of hunting differs from that of call forwarding. Hunting allows Cisco Unified CallManager to extend a call to one or more lists of numbers, where each such list can specify a hunting order that is chosen from a fixed set of algorithms. When a call extends to a hunt party from these lists and the party fails to answer or is busy, hunting resumes with the next hunt party. (The next hunt party varies depending on the current hunt algorithm.) Hunting thus ignores the Call Forward No Answer (CFNA), Call Forward Busy (CFB), or Call Forward All (CFA) settings for the attempted party.

Call forwarding allows detailed control as to how to extend (*divert* and *redirect* represent equivalent terms for *extend*) a call when a called party fails to answer or is busy and hunting is not taking place. For example, if the CFNA setting for a line is set to a hunt-pilot number, a call to that line that is not answered diverts to the hunt-pilot number and thus begins hunting.

Starting with Release 4.1 of Cisco Unified CallManager, Cisco Unified CallManager offers the ability to redirect a call when hunting fails (that is, when hunting terminates without any hunt party answering, due either to exhausting the list of hunt numbers or to timing out). If used, this final redirection comprises a Call Forwarding action. Therefore, the Hunt Pilot Configuration window includes Call Forwarding configuration concepts that are similar to those found on the Directory Number Configuration window.

Example of Call Hunting

Although hunting differs from forwarding, hunting often originates as a call that gets forwarded to a hunt-pilot number. The call coverage feature extends hunting to allow final forwarding after hunting either exhausts or times out.

A typical call that invokes hunting can include the following phases:

1. A call extends to the original called party.
2. The call forwards to hunting (for example, due to the Call Forward All [CFA], CFNA, or CFB setting for the original called line).
3. The call hunts through provisioned hunt groups according to provisioned algorithms for each group. Hunting either succeeds (if a hunt party answers), exhausts (if all hunt parties are attempted, but none answer), or times out (if the time specified in the Maximum Hunt Timer runs out before all parties are attempted, and none of the parties that were attempted answer).

   For the purpose of this example, we assume that hunting does not succeed.
4. If some form of final forwarding is configured, the call forwards to a next destination; otherwise, the call gets released.

Maximum Hunt Timer

The Maximum Hunt Timer field on the Hunt Pilot Configuration window allows the administrator to enter a value (in seconds) to limit the time for hunting through a hunt list. After the specified time lapses, if hunting has not succeeded, the call gets forwarded to a voice-messaging system, a specific dialed number, or some personal treatment (if configured), or the call gets released.

For more details about the Maximum Hunt Timer, refer to the field description in the "Hunt Pilot Configuration" section of the *Cisco Unified CallManager Administration Guide*.

Internal and External Calls

Forwarding provides separate configuration based on whether the originator of a call is an internal user or an external user. This distinction applies to Call Forward Busy (CFB), Call Forward No Answer (CFNA), and Call Forward No Coverage (CFNC) cases.

Personal Preferences

Hunting supports the capability to provide a final forwarding treatment to voice-messaging system, a specific dialed number, or some personal treatment (based on the original called party) when hunting either exhausts or times out. The capability to provide separate final forwarding treatment based on whether the call was internal or external also exists. Hunting supports a separate, configurable maximum hunt timer for each hunt-pilot number.

In the Hunt Pilot configuration settings, Use Personal Preferences Destination fields are available to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to the hunt pilot. Refer to the "Hunt Pilot Configuration Settings" section in the *Cisco Unified CallManager Administration Guide*.

Closest Match Routing

Closest match routing process routes a call by using the route pattern that most closely matches the dialed number. When the Cisco Unified CallManager encounters a dialed number that matches multiple route patterns, it uses closest match routing to determine which route pattern most closely matches the number and directs the call by using that route pattern.

When two configured route patterns exactly match the same number of addresses in different partitions, Cisco Unified CallManager chooses the route pattern on the basis of the order in which the partitions are listed in the calling search space. (Cisco Unified CallManager chooses the route pattern from the partition that appears first in the calling search space.)

If two configured route patterns exactly match the same number of addresses in a partition, the Cisco Unified CallManager arbitrarily chooses one. The following paragraphs explain why such exact matches signify an unusual occurrence.

Several route patterns can match a single number. For instance, the number 8912 matches all the following route patterns: 8912, 89XX, and 8XXX.

In this example, the route pattern 8912 matches exactly one address. The route pattern 89XX matches 8912 plus 99 other addresses, and the route pattern 8XXX matches 8912 plus 999 other addresses.

If the user dials 8913, the call routes differently. Using the preceding example, this address matches only the routing patterns 89XX and 8XXX. Because 89XX matches a narrower range of addresses than 8XXX, the Cisco Unified CallManager delivers the call to the device that is assigned the routing pattern 89XX.

Using the @ Wildcard Character in Route Patterns

Using the @ wildcard character in a route pattern provides a single route pattern to match all NANP numbers, and requires additional consideration.

The number 92578912 matches both of the following route patterns: 9.@ and 9.XXXXXXX. Even though both these route patterns seem to equally match the address, the 9.@ route pattern actually provides the closest match. The @ wildcard character encompasses many different route patterns, and one of those route patterns is [2-9][02-9]XXXXX. Because the number 2578912 more closely matches [2-9][02-9]XXXXX than it does XXXXXXX, the 9.@ route pattern provides the closest match for routing.

When configuring route patterns, take the following considerations into account:

- When @ is used in a routing pattern, the system recognizes octothorpe (#) automatically as an end-of-dialing character for international calls. For routing patterns that do not use @, you must include the # in the routing pattern to be able to use the # character to signal the end of dialing.
- If the route pattern contains an at symbol (@), the Discard Digits field can specify any discard digits instructions (DDIs).

  The "Special Characters and Settings" section on page 17-15 lists DDIs and describes the effects of applying each DDI to a dialed number.

Discard Digits Instructions

A discard digits instruction (DDI) removes a portion of the dialed digit string before passing the number on to the adjacent system. Portions of the digit string must be removed, for example, when an external access code is needed to route the call to the PSTN, but the PSTN switch does not expect that access code.

Note With non-@ patterns, you can use only Discard Digits instructions <None>, NoDigits, and PreDot.

Static Digit Analysis

Prior to Release 4.0 of Cisco Unified CallManager, unregistered devices without configured forwarding got removed from the digit analysis (DA) table and required dynamic digit analysis. Prior to Release 4.0, when a phone unregistered, call processing allowed a call to pass to the next closest match in the Calling Search Space (CSS) list. With the introduction of static DA in Release 4.0, whether a phone is registered or not, the device remains in the DA table, and the directory number intercepts the call.

Configuration Tip

- Administrators should note that Cisco Unified CallManager Assistant does not use translation patterns for failover. Instead, administrators must set up Call Forward No Answer (CFNA) with the data that was in the translation pattern for all Unified CM Assistant failed route points, and these route points must be removed.

Beginning with Release 4.0 of Cisco Unified CallManager, the digit analysis process builds a static digit analysis engine with the patterns that are configured in the database during system initialization. This digit analysis engine reduces the propagation of patterns within a cluster of Cisco Unified CallManagers and makes Cisco Unified CallManager more scalable.

In previous releases, the individual device control process read pattern information from the database and dynamically registered the patterns to the digit analysis process to build its digit analysis engine. Each pattern had a mapping to its control process ID in the digit analysis engine. The control process ID of a pattern got changed dynamically if its associated device was reset or if a Cisco Unified CallManager server restarted. If a change to the control process ID took place, the digit analysis engine had to be changed dynamically, and its contents required propagation to other Cisco Unified CallManager servers. During call processing, the digit analysis engine returned the control process ID of a matched pattern.

Beginning with Release 4.0 of Cisco Unified CallManager, the digit analysis process reads the pattern information directly from the database to build the static digit analysis engine during Cisco Unified CallManager initialization. With the static digit analysis engine, each pattern has a mapping to its callable endpoint name, which is a NumPlanPkID of the pattern in the database, a unique identifier to a configured pattern in Cisco Unified CallManager. The static digit analysis engine no longer holds the control process ID of a pattern.

Static digit analysis integrates with the changes to the device manager to support all existing functions and features. The device manager includes a table where a NumPlanPkID shows a one-to-one mapping to the control process ID of a pattern. When processing a call, digit analysis asks the device manager to get the control process ID for a matched pattern.

Feature Description

Cisco Unified CallManager includes these pattern types: Call Park, Call Forward, Meet-Me Conference, Device, Translation, Call Pickup Group, Route, and Message Waiting. The Device, Translation, and Route pattern types represent static patterns. The digit analysis process reads these patterns directly and inserts them into the static digit analysis engine during the initialization of a Cisco Unified CallManager.

Other pattern types (Call Park, Call Forward, Meet-Me Conference, Call Pickup Group, and Message Waiting), which are intercept patterns, remain dynamic patterns. Their individual control process reads the pattern information from the database and then asks the digit analysis process to insert the pattern into the static digit analysis engine via registration messages.

All static patterns remain unchanged until their records are changed in the database. Static patterns do not require propagation because the database change notification is broadcast to the servers within a cluster. Dynamic patterns still use the existing propagating and updating mechanism to update the static digit analysis engines.

Regardless of its pattern type, each static pattern in the static digit analysis engine has a mapping to its PkID in the NumPlan table in the database. When a device registers its patterns to the device manager, the same PkID gets saved and mapped to its control process ID in the device manager. A new interface between the digit analysis and device manager retrieves the control process ID when a matched pattern is found in the static digit analysis engine during call processing.

Caveat 1

A potential loss of change notification exists in the current Cisco Unified CallManager release. This loss could cause a device that is registered with Cisco Unified CallManager to become unreachable by other devices. The following paragraphs provide troubleshooting for this potential problem.

The most common cause for this problem occurs when the DN that is assigned to the device belongs to a partition that is not contained in the calling search space of other devices. If the calling search space of other devices does contain the partition for that DN, other reasons may apply. For example, the DN changed only for that device, and the change notification from the database to Cisco Unified CallManager was lost. Beginning with Release 4.0 of Cisco Unified CallManager, resetting the device may not resolve the problem.

To resolve this problem, remove the DN and add the DN to the system again. Remove the DN from its device on the Directory Number Configuration window and on the Route Plan Report window. After you remove the DN, add it back in with the same partition, pattern, and other configuration information. The process should resolve the problem after you add the new DN to Cisco Unified CallManager again.

The same workaround applies to route patterns and translation patterns if similar problems exist.

Tip Be sure to document all configurations before removing the patterns.

Caveat 2

Static digit analysis disables the configuration of several applications. These applications rely on the provision of duplicate patterns in the same calling search space. For example, the CTI application may be pattern 5000 in partition A, and a particular phone may be pattern 5000 in partition B. In previous releases, if the CTI route point is down, the phone will ring. With static digit analysis, however, the caller receives a busy tone. This limitation implies that the application failure does not get handled.

Administrators would normally use Call Forward No Answer and Call Forward on failure to handle application failure, but when the pattern on the CTI route point is 5XXX, you cannot configure a forward destination of 5XXX. To resolve this limitation, you can now perform configuration of X characters in Call Forward destinations.

The following example demonstrates the functionality of digit analysis prior to Release 4.0 (with dynamic digit analysis) and in Release 4.0 and subsequent releases (with static digit analysis) for the Cisco Unified CallManager Assistant application.

IPMA Example with Digit Analysis Prior to Release 4.0

Given the following configuration

```
Partitions: IPMA, Managers, Everyone
CSS-I-E: IPMA:Everyone
CSS-M-E: Managers:Everyone
Line-1/CSS-I-E: EveryOne/1000
Line-2/CSS-M-E: Manager/1001
CTI RP: IPMA/1XXX
Translation Pattern/CSS-M-E: EveryOne/1XXX
```

If the CTI route point (RP) is up, 1000/IPMA:EveryOne calls 1001. The call routes by using the CTI route point *IPMA/1XXX*.

If the CTI route point is down, 1000/IPMA:EveryOne calls 1001. The call goes through the translation pattern *Everyone/1xxx,* and the call reaches Manager/1001 after the translation and achieves the goal of the IPMA application.

Cisco Unified CallManager Assistant Example with Static Digit Analysis in Release 4.0 and Subsequent Releases

Given an identical configuration, in Release 4.0 and in subsequent releases, you must make the following modification: configure *1xxx* as a CFNA mask and CSS-E as a CFNA calling search space for the CTI route point to handle the CTI route point failure case.

When static digit analysis gets used, the following processing takes place:

- If the CTI route point (RP) is up, 1000/IPMA:EveryOne calls 1001. The call routes through CTI route point *IPMA/1XXX*. (Routing does not change from previous releases.)
- If the CTI route point is down, 1000/IPMA:EveryOne calls 1001. The call goes to the CTI route point, and its CFNA is triggered. The forwarding feature routes the call through the translation pattern *Everyone/1xxx*, and the call reaches Manager/1001 after translation.

Without configuring the CFNA in the CTI route point, the translation pattern never gets matched, and the Cisco Unified CallManager Assistant application fails.

Special Characters and Settings

Cisco Unified CallManager Administration allows you to use special characters and settings to perform the following tasks:

- Allowing a single route pattern or hunt pilot to match a range of numbers
- Removing a portion of the dialed digit string
- Manipulating the appearance of the calling party number for outgoing calls
- Manipulating the dialed digits, or called party number, for outgoing calls

For more information on how to use special characters and settings, see the following topics:

- Wildcards and Special Characters in Route Patterns and Hunt Pilots, page 17-16
- Discard Digits Instructions, page 17-18

Wildcards and Special Characters in Route Patterns and Hunt Pilots

Wildcards and special characters in route patterns and hunt pilots allow a single route pattern or hunt pilot to match a range of numbers (addresses). Use these wildcards and special characters also to build instructions that enable the Cisco Unified CallManager to manipulate a number before sending it to an adjacent system.

Table 17-3 describes the wildcards and special characters that Cisco Unified CallManager supports.

Table 17-3 Wildcards and Special Characters

Character	Description	Examples
@	The at symbol (@) wildcard matches all NANP numbers. Each route pattern can have only one @ wildcard.	The route pattern 9.@ routes or blocks all numbers that the NANP recognizes. The following route patterns examples show NANP numbers that the @ wildcard encompasses: • 0 • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	The X wildcard matches any single digit in the range 0 through 9.	The route pattern 9XXX routes or blocks all numbers in the range 9000 through 9999.
!	The exclamation point (!) wildcard matches one or more digits in the range 0 through 9.	The route pattern 91! routes or blocks all numbers in the range 910 through 9199999999999999999999.
?	The question mark (?) wildcard matches zero or more occurrences of the preceding digit or wildcard value.	The route pattern 91X? routes or blocks all numbers in the range 91 through 9199999999999999999999.
+	The plus sign (+) wildcard matches one or more occurrences of the preceding digit or wildcard value.	The route pattern 91X+ routes or blocks all numbers in the range 910 through 9199999999999999999999.
[ ]	The square bracket ([ ]) characters enclose a range of values.	The route pattern 813510[012345] routes or blocks all numbers in the range 8135100 through 8135105.
-	The hyphen (-) character, used with the square brackets, denotes a range of values.	The route pattern 813510[0-5] routes or blocks all numbers in the range 8135100 through 8135105.
^	The circumflex (^) character, used with the square brackets, negates a range of values. Ensure that it is the first character following the opening bracket ([). Each route pattern can have only one ^ character.	The route pattern 813510[^0-5] routes or blocks all numbers in the range 8135106 through 8135109.

Table 17-3 Wildcards and Special Characters (continued)

Character	Description	Examples
.	The dot (.) character, used as a delimiter, separates the Cisco Unified CallManager access code from the directory number. Use this special character, with the discard digits instructions, to strip off the Cisco Unified CallManager access code before sending the number to an adjacent system. Each route pattern can have only one dot (.) character.	The route pattern 9.@ identifies the initial 9 as the Cisco Unified CallManager access code in an NANP call.
*	The asterisk (*) character can provide an extra digit for special dialed numbers.	You can configure the route pattern *411 to provide access to the internal operator for directory assistance.
#	The octothorpe (#) character generally identifies the end of the dialing sequence. Ensure the # character is the last character in the pattern.	The route pattern 901181910555# routes or blocks an international number that is dialed from within the NANP. The # character after the last 5 identifies this digit as the last digit in the sequence.

Table 17-4 lists Cisco Unified CallManager Administration fields that require route patterns or hunt pilots and shows the valid entries for each field.

Table 17-4 Field Entries

Field	Valid entries
Call Park Number/Range	[^ 0 1 2 3 4 5 6 7 8 9 -] X * #
Calling Party Transform Mask	0 1 2 3 4 5 6 7 8 9 X A B C D * #
Called Party Transform Mask	0 1 2 3 4 5 6 7 8 9 X A B C D * #
Caller ID DN (Gateways)	0 1 2 3 4 5 6 7 8 9 X * #
Directory Number	[^ 0 1 2 3 4 5 6 7 8 9 -] + ? ! X * # +
Directory Number (Call Pickup Group)	0 1 2 3 4 5 6 7 8 9
External Phone Number Mask	0 1 2 3 4 5 6 7 8 9 X * #
Forward All	0 1 2 3 4 5 6 7 8 9 * #
Forward Busy	0 1 2 3 4 5 6 7 8 9 * #
Forward No Answer	0 1 2 3 4 5 6 7 8 9 * #
Meet-Me Conference Number	[^ 0 1 2 3 4 5 6 7 8 9 -] X * #
Prefix Digits	0 1 2 3 4 5 6 7 8 9 A B C D * #
Prefix DN (Gateways)	0 1 2 3 4 5 6 7 8 9 * #
Route Filter Tag Values	[^ 0 1 2 3 4 5 6 7 8 9 -] X * #
Route Pattern	[^ 0 1 2 3 4 5 6 7 8 9 A B C D -] + ? ! X * # + . @

Table 17-4 Field Entries (continued)

Field	Valid entries
Translation Pattern	[^ 0 1 2 3 4 5 6 7 8 9 A B C D -] + ? ! X * # + . @
Hunt Pilot	[^ 0 1 2 3 4 5 6 7 8 9 A B C D -] + ? ! X * # + . @

Discard Digits Instructions

A discard digits instruction (DDI) removes a portion of the dialed digit string before passing the number on to the adjacent system. A DDI must remove portions of the digit string, for example, when an external access code is needed to route the call to the PSTN, but the PSTN switch does not expect that access code.

Table 17-5 lists DDIs and describes the effects of applying each DDI to a dialed number.

Table 17-5 Discard Digits Instructions

DDI	Effect	Example
10-10-Dialing	This DDI removes • IXC access code	Route pattern: 9.@ Dialed digit string: 9101028897281350000 After applying DDI: 99728135000
10-10-Dialing Trailing-#	This DDI removes • IXC access code • End-of-dialing character for international calls	Route pattern: 9.@ Dialed digit string: 91010288011819105555# After applying DDI: 901181910555
11/10D->7D	This DDI removes • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 9.@ Dialed digit string: 919728135000 or 99728135000 After applying DDI: 98135000

Table 17-5 Discard Digits Instructions (continued)

DDI	Effect	Example
11/10D->7D Trailing-#	This DDI removes • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code • End-of-dialing character for international calls This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 9.@ Dialed digit string: 919728135000 or 99728135000 After applying DDI: 98135000
11D->10D	This DDI removes • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code	Route pattern: 9.@ Dialed digit string: 919728135000 After applying DDI: 99728135000
11D->10D Trailing-#	This DDI removes • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • End-of-dialing character for international calls • IXC access code	Route pattern: 9.@ Dialed digit string: 919728135000 After applying DDI: 99728135000
Intl TollBypass	This DDI removes • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code	Route pattern: 9.@ Dialed digit string: 901181910555 After applying DDI: 9910555
Intl TollBypass Trailing-#	This DDI removes • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code • End-of-dialing character	Route pattern: 9.@ Dialed digit string: 901181910555# After applying DDI: 9910555

Table 17-5 Discard Digits Instructions (continued)

DDI	Effect	Example
NoDigits	This DDI removes no digits.	Route pattern: 9.@ Dialed digit string: 919728135000 After applying DDI: 919728135000
Trailing-#	This DDI removes • End-of-dialing character for international calls	Route pattern: 9.@ Dialed digit string: 901181910555# After applying DDI: 901181910555
PreAt	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code	Route pattern: 8.9@ Dialed digit string: 899728135000 After applying DDI: 9728135000
PreAt Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 8901181910555# After applying DDI: 01181910555
PreAt 10-10-Dialing	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • IXC access code	Route pattern: 8.9@ Dialed digit string: 89101028897281350000 After applying DDI: 9728135000
PreAt 10-10-Dialing Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • IXC access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 89101028801181910555# After applying DDI: 01181910555

Table 17-5 Discard Digits Instructions (continued)

DDI	Effect	Example
PreAt 11/10D->7D	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 8.9@ Dialed digit string: 8919728135000 or 899728135000 After applying DDI: 8135000
PreAt 11/10D->7D Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code • End-of-dialing character for international calls This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 8.9@ Dialed digit string: 8919728135000 or 899728135000 After applying DDI: 8135000
PreAt 11D->10D	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code	Route pattern: 8.9@ Dialed digit string: 8919728135000 After applying DDI: 9728135000

Table 17-5 Discard Digits Instructions (continued)

DDI	Effect	Example
PreAt 11D->10D Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 8919728135000 After applying DDI: 9728135000
PreAt Intl TollBypass	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code	Route pattern: 8.9@ Dialed digit string: 8901181910555 After applying DDI: 910555
PreAt Intl TollBypass Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code • End-of-dialing character	Route pattern: 8.9@ Dialed digit string: 8901181910555# After applying DDI: 910555

Table 17-5 Discard Digits Instructions (continued)

DDI	Effect	Example
PreDot	This DDI removes • Cisco Unified CallManager external access code	Route pattern: 8.9@ Dialed digit string: 899728135000 After applying DDI: 99728135000
PreDot Trailing-#	This DDI removes • Cisco Unified CallManager external access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 8901181910555# After applying DDI: 901181910555
PreDot 10-10-Dialing	This DDI removes • Cisco Unified CallManager external access code • IXC access code	Route pattern: 8.9@ Dialed digit string: 891010288972813500 0 After applying DDI: 99728135000
PreDot 10-10-Dialing Trailing-#	This DDI removes • Cisco Unified CallManager external access code • IXC access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 89101028801181910555# After applying DDI: 901181910555
PreDot 11/10D->7D	This DDI removes • Cisco Unified CallManager external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 8.9@ Dialed digit string: 8919728135000 or 899728135000 After applying DDI: 98135000

Table 17-5 Discard Digits Instructions (continued)

DDI	Effect	Example
PreDot 11/10D->7D Trailing-#	This DDI removes • Cisco Unified CallManager external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code • End-of-dialing character for international calls This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 8.9@ Dialed digit string: 8919728135000 or 899728135000 After applying DDI: 98135000
PreDot 11D->10D	This DDI removes • Cisco Unified CallManager external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code	Route pattern: 8.9@ Dialed digit string: 8919728135000 After applying DDI: 99728135000
PreDot 11D->10D Trailing-#	This DDI removes • Cisco Unified CallManager external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 8919728135000 After applying DDI: 99728135000

Table 17-5 Discard Digits Instructions (continued)

DDI	Effect	Example
PreDot Intl TollBypass	This DDI removes • Cisco Unified CallManager external access code • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code	Route pattern: 8.9@ Dialed digit string: 8901181910555 After applying DDI: 9910555
PreDot Intl TollBypass Trailing-#	This DDI removes • Cisco Unified CallManager external access code • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code • End-of-dialing character	Route pattern: 8.9@ Dialed digit string: 8901181910555# After applying DDI: 9910555

Calling and Called Party Transformations

Cisco Unified CallManager Administration allows you to manipulate the calling party number and the called party number that Cisco Unified CallManager sends with each call setup message.

The following topics provide information on these settings:

- Calling Party Number Transformations Settings, page 17-25
- Called Party Number Transformations Settings, page 17-27

Calling Party Number Transformations Settings

Calling party transformations settings allow you to manipulate the appearance of the calling party number for outgoing calls. Cisco Unified CallManager uses the calling party number for calling line identification (CLID). During an outgoing call, the CLID passes to each private branch exchange (PBX), central office (CO), and interexchange carrier (IXC) as the call progresses. The called party receives the calling line identification (CLID) when the call is offered to the called party.

Configuration for calling party transformations settings that are used in route lists occurs in the individual route groups that comprise the list. The calling party transformations settings that are assigned to the route groups in a route list override any calling party transformations settings that are assigned to a route pattern that is associated with that route list.

You can set the following calling party transformation settings in the route group configuration:

- Use Calling Party's External Phone Number Mask
- Calling Party Transform Mask
- Prefix Digits (Outgoing Calls)

Table 17-6 describes the fields, options, and values that are used to specify calling party number transformations.

Table 17-6 Calling Party Number Transformations Settings

Field Name	Description
Use Calling Party’s External Phone Number Mask	This field determines whether the full, external phone number is used for calling line identification (CLID) on outgoing calls. (Configure the external number by using the Directory Number Configuration window.) You can set the following Calling Party Transformations settings for the route group by clicking the members in the Route List Details panel of the Route List Configuration window: • Default: This setting indicates that the route group does not govern the calling party external phone number and calling party transform masks. If a calling party external phone number mask or transform mask is chosen for the route pattern, calls that are routed through this route group use those masks. • Off: This setting indicates that the calling party external phone number is not used for CLID. If no transform mask is entered for this route group, calls that are routed through this group do not get associated with a CLID. • On: This setting indicates that the calling party full, external number is used for CLID. The external phone number mask can contain up to 24 digits.
Calling Party Transform Mask	This field specifies the calling party transform mask for all calls that are routed through this route group. Valid values for this field range from 0 through 9, the wildcard character X, and the characters * and #. You can also leave this field blank. If it is blank and the preceding field is set to Off, this means that no calling party number is available for CLID. The calling party transform mask can contain up to 50 digits.
Prefix Digits (Outgoing Calls)	This field contains a prefix digit or a set of Prefix Digits (Outgoing Calls) that are appended to the calling party number on all calls that are routed through this route group. Valid values for this field range from 0 through 9, the characters * and #, and blank. Prefix Digits (Outgoing Calls) can contain up to 50 digits on route patterns or up to 24 digits on DNs.

Called Party Number Transformations Settings

Called party transformations settings allow you to manipulate the dialed digits, or called party number, for outgoing calls. Examples of manipulating called numbers include appending or removing prefix digits (outgoing calls), appending area codes to calls dialed as seven-digit numbers, appending area codes and office codes to interoffice calls dialed as four- or five-digit extensions, and suppressing carrier access codes for equal access calls.

Configuration of called party transformations settings that are used in route lists occurs in the individual route groups that comprise the list. The called party transformations settings that are assigned to the route groups in a route list override any called party transformations settings that are assigned to a route pattern or translation pattern that is associated with that route list.

You can set the following called party transformation settings in the route group, route pattern, and translation pattern configuration:

- Discard Digits
- Called Party Transform Mask
- Prefix Digits (Outgoing Calls)

Table 17-7 describes the fields, options, and values that are used to specify called party number transformations.

Table 17-7 Called Party Number Transformations Settings

Field Name	Description
Route Group Configuration	
Discard Digits	This field contains a list of discard patterns that control the discard digit instructions. For example, in a system where users must dial 9 to make a call to the public switched telephone network (PSTN), the PreDot discard pattern causes the 9 to be stripped from the dialed digit string. See the "Closest Match Routing" section on page 17-12 for more information. **Note** Any setting other than the default setting of <None> overrides the setting in the route pattern. The <None> setting means "do not discard digits."
Called Party Transform Mask	This field specifies the called party transform mask for all calls that are routed through this route group. Valid values for this field range from 0 through 9, the wildcard character X, and characters * and #. You can also leave this field blank. If this field is blank, no transformation takes place; Cisco Unified CallManager sends the dialed digits exactly as dialed. The called party transform mask can contain up to 50 digits.
Prefix Digits (Outgoing Calls)	This field contains a prefix digit or a set of Prefix Digits (Outgoing Calls) that are appended to the called party number on all calls that are routed through this route group. Valid values for this field range from 0 through 9, the characters * and #, and blank. Prefix Digits (Outgoing Calls) can contain up to 50 digits on route patterns or up to 24 digits on DNs.

Related Topics

- Special Characters and Settings, page 17-15
- Closest Match Routing, page 17-12

- Caller Identification and Restriction, page 17-28
- Understanding Route Plans, page 17-1

Caller Identification and Restriction

Cisco Unified CallManager provides the following types of caller identification information:

- Calling Line Identification (CLID)—Provides the called party with the calling party's extension or directory number on a display.
- Calling Name Identification—Provides the called party with the calling party's name on a display.
- Connected Line Identification—Provides the calling party with the connected party's phone number on a display.
- Connected Name Identification—Provides the calling party with the connected party's name on a display

Cisco CallManger provides flexible configuration options to allow and to restrict the display of the line and name information for both calling and connected parties.

For more information on how to use caller identification settings, see the following topics:

- Calling Party Presentation and Restriction Settings, page 17-28
- Connected Party Presentation and Restriction Settings, page 17-30

Calling Party Presentation and Restriction Settings

Calling party presentation information controls whether to display the phone number and name information that Cisco Unified CallManager sends with setup messages for an outgoing call. Cisco Unified CallManager uses the following fields to provide these supplementary services:

- Calling Line ID Presentation field—Calling line identification presentation (CLIP) or calling line identification restriction (CLIR)
- Calling Name Presentation field—Calling name presentation (CNIP) or calling name restriction (CNIR)

You can use the Calling Line ID Presentation field in the Gateway Configuration window to control whether the CLID displays for all outgoing calls on the gateway. To control the CLID display on a call-by-call basis, you use the Calling line ID Presentation field in Route Pattern Configuration or Translation Pattern Configuration windows.

Note Configure Calling Line ID Presentation and Connected Line ID Presentation, in combination with the Ignore Presentation Indicators (internal calls only) device-level parameter, to set up call display restrictions. Together, these settings allow you to selectively present or block calling and/or connected line display information for each call. For more information about the Ignore Presentation Indicators (internal calls only) field, refer to the Device Profile Configuration chapter and the Cisco Unified IP Phone Configuration chapter in the *Cisco Unified CallManager Administration Guide*. For more information about call display restrictions, refer to the Call Display Restrictions chapter in the *Cisco Unified CallManager Features and Services Guide*.

The following example describes how calling line ID presentation works. When a user makes a call, Cisco Unified CallManager checks whether the dialed number matches a translation pattern. Cisco Unified CallManager finds a match and sets the presentation indicator to the value in the translation pattern Calling Line ID Presentation field, which specifies "restricted" in this example. Next, Cisco Unified CallManager checks and finds a match on a route pattern that is configured for the dialed number. Cisco Unified CallManager checks the Calling Line ID Presentation field and finds that the value specifies "default." The presentation indicator remains as "restricted" because the previous setting is unchanged when default is set.

The gateway Calling Line ID Presentation field gets checked last. In this example, the value specifies "allowed" and overrides the previous calling line ID presentation indicator to allow the calling party number to display on the called party phone. Therefore, the calling line ID presentation field indicator changed from "restricted" at the time that the calling party initiated the call to "allowed" by the time that Cisco Unified CallManager sends the call setup message to the endpoint device.

You can configure line and name presentation or restriction on a call-by-call basis for outgoing calls and incoming calls by using the Route Pattern Configuration or Translation Pattern Configuration pages.

For the gateway, you can only configure calling line ID presentation for outgoing calls. For incoming calls, Cisco Unified CallManager uses the Connected Line ID Presentation field for the gateway to specify whether to allow or restrict the connected party number to display on the calling party phone. Gateway settings only apply in these two situations, and these settings override all other settings. For the gateway, you can only configure calling and connected line presentation. No settings exist to control name presentation on the gateway.

The type of device control protocol that handles the call limits caller name and number information. See Table 17-10 for a list of protocols with the supported caller name and number information.

Note To control the name display for non-QSIG trunks, you must enable the Display IE Delivery field or Send Calling Name in Facility IE field in the Gateway Configuration window.

Table 17-8 describes the fields, options, and values that are used to specify calling party presentations.

Table 17-8 Calling Party Presentation Settings

Field Name	Description
Calling Line ID Presentation (outgoing call)	This field determines whether the calling party phone number displays on the called party phone display screen. The Gateway Configuration, the Route Pattern Configuration, and the Translation Pattern Configuration windows use the Calling Line Presentation field. The following list gives the options for this field: • Default: If default is set, calling line ID presentation does not get modified. • Allowed: Use this setting to permit the calling party phone number to display in the called party phone display. • Restricted: Use this setting to display "Private" in the called party phone display and block the display of the calling party phone number.

Table 17-8 Calling Party Presentation Settings (continued)

Field Name	Description
Calling Name Presentation (outgoing call)	This field determines whether the calling party's name displays on the called party phone display. The Route Pattern Configuration and Translation Pattern Configuration windows use the Calling Name Presentation field. The following list gives the options for this field: • Default: If default is set, calling name presentation does not get modified. • Allowed: Use this setting to display the calling party name in the called party phone display. • Restricted: Use this setting in the route patterns or translation patterns configuration displays "Private" in the called party phone display. **Note** The gateway has no setting for calling name presentation.
Calling Line ID Presentation (incoming call)	If the incoming call goes through a translation pattern or route pattern and the calling line ID presentation setting is allowed or restricted, the calling line presentation gets modified with the translation or route pattern setting. If the call comes into the Cisco Unified CallManager system and then goes out to a PBX or the PSTN, the outgoing call rules apply as stated in the "Calling Party Presentation and Restriction Settings" section on page 17-28. **Note** The gateway calling line ID presentation setting controls outgoing calls only.
Calling Name Presentation (incoming call)	If the incoming call goes through a translation pattern or route pattern and the calling name presentation setting is allowed or restricted, the calling name presentation gets modified with the translation or route pattern setting. If the call comes into the Cisco Unified CallManager system and then goes out to a PBX or the PSTN, the outgoing call rules apply as stated in the "Calling Party Presentation and Restriction Settings" section on page 17-28. **Note** The gateway has no settings to control name information.

Connected Party Presentation and Restriction Settings

Connected party presentation information controls whether to display the phone number and name information that Cisco Unified CallManager receives with an incoming call. Cisco Unified CallManager uses the following fields to provide these supplementary services:

- Connected Line ID Presentation field—Connected line identification presentation (COLP) or connected line identification restriction (COLR)
- Connected Name Presentation field—Connected name presentation (CONP) or calling name restriction (CONR)

Connected party settings allow you to display or restrict the display of the phone number and name of the connected party on the calling party's phone. Translation Pattern Configuration and Route Pattern Configuration windows include these two settings. The calling party receives the connected name information after the call connects to Cisco Unified CallManager and the terminating phone.

The following example describes how connected line ID works. When Cisco Unified CallManager receives an incoming call, it checks whether a translation pattern is configured for the incoming number. Cisco Unified CallManager uses the value in the Connected Line ID Presentation field that specifies "restricted" for this example. Next, if a route pattern is configured for the incoming call, the value in the Connected Line ID Presentation field gets checked. In this example, the value specifies "default," so the indicator remains as "restricted," which prevents the connected party number from displaying on the calling party's phone.

For incoming calls only, the gateway Connected Line ID Presentation field value gets checked last and is set for "allowed" in this example. The gateway setting specifies whether the connected party number can display on the calling party phone. In this case, Cisco Unified CallManager sends "allowed" in the CONNECT message, so the connected line can display on the originating caller's phone display.

You can configure connected line and name presentation or restriction on a call-by-call basis for outgoing calls and incoming calls by using the Route Pattern Configuration or Translation Pattern Configuration windows.

For incoming calls on the gateway, you use the Connected Line ID Presentation field to specify whether to allow or restrict the display of the connected party number on the calling party's phone. Gateway settings only apply to line presentation settings and override all other settings.

Note For the gateway, you can only configure calling and connected line presentation options. No settings exist for name presentation on the gateway.

Table 17-9 describes the fields, options, and values that are used to specify connected party presentations.

Table 17-9 Connected Party Presentation Settings

Field Name	Description
Connected Line ID Presentation (outgoing call)	In the Route Pattern Configuration and the Translation Pattern Configuration windows, this field determines whether the connected party number displays on the calling party phone display. The following list gives the options for this field: • Default: If default is set, connected line ID presentation does not get modified. • Allowed: Use this setting to display the connected line number that Cisco Unified CallManager received in protocol messages on the calling party phone display. • Restricted: Use this setting to block the connected party number from displaying in the calling party phone display, and "Unknown Number" displays instead. **Note** This setting applies to internal calls and calls on QSIG connections only.

Table 17-9 Connected Party Presentation Settings (continued)

Field Name	Description
Connected Name Presentation (CONP/CONR) (outgoing call)	This field determines whether the connected party name displays on the calling party phone display. The Route Pattern Configuration and Translation Pattern Configuration windows use the Connected Name Presentation field. The following list gives the options for this field: • Default: If default is set, calling name presentation does not get modified. • Allowed: Use this setting to display the connected party name that Cisco Unified CallManager received in protocol messages in the calling party phone display. • Restricted: Use this setting to block the connected party name from displaying, and display "Unknown" in the calling party phone display.
Connected Line ID Presentation (incoming call)	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 connected line presentation indicator gets modified with the translation or route pattern setting. **Note** The Connected Line ID Presentation setting on the gateway determines if the connected party number can display on the originating party's phone. If the call comes into the Cisco Unified CallManager system and then goes out to a PBX or the PSTN, the outgoing call rules apply as stated in the "Connected Party Presentation and Restriction Settings" section on page 17-30.
Connected Name Presentation (incoming call)	If the incoming call goes through a translation or route pattern and the connected name presentation setting is set to allowed or restricted, the connected name presentation gets modified with the translation or route pattern setting. If the call comes into the Cisco Unified CallManager system and then goes out to a PBX or the PSTN, the outgoing call rules apply as stated in the "Connected Party Presentation and Restriction Settings" section on page 17-30. **Note** The gateway has no settings to control name information.

Caller Identification Support with Device Control Protocols in Cisco Unified CallManager

Cisco Unified CallManager provides support for caller name and number identification presentation based on the device control protocols that handle the call. Not all device protocols provide caller number and name information in the protocol messages. Table 17-10 summarizes which protocols support caller identification services.

Table 17-10 Caller Identification Information Supported by Device Control Protocols

Device Control Protocol	Calling Line	Calling Name	Connected Line	Connected Name
IP Phones with SCCP	provides line number	provides name associated with DN	displays number when received	displays name when received
MGCP Stations (FXS)	provides line number	provides name associated with DN	not supported	displays name when received
MGCP Trunk (FXO, T1 CAS)	not supported	not supported	not supported	not supported
H.323 Trunk	calling line sent in H.225 SETUP	supported by using DISPLAY IE in H.225 messages for intercluster trunks only	supported by H.225 NOTIFY for intercluster trunks only	supported by DISPLAY IE in H.225 messages for intercluster trunks only
PRI Trunk	calling line in PRI SETUP	supported by using FACILITY IE in PRI messages	not supported	supported by using FACILITY IE in PRI messages
QSIG Trunk	calling line in QSIG SETUP	supported by using FACILITY IE in QSIG messages	supported by QSIG CONNECT	supported by using FACILITY IE in QSIG messages
SIP Trunk	calling line included in From and Remote-Party- ID headers	calling name included in From and Remote-Party-ID headers	connected line included in Remote-Party-ID header	connected name included in Remote-Party-ID header

Related Topics

- Calling and Called Party Transformations, page 17-25
- Special Characters and Settings, page 17-15
- Enhanced Call Identification Services, page 41-9

External Route Plan Wizard

The external route plan wizard generates a single-tenant, multilocation, partitioned route plan for the North American Numbering Plan (NANP) area by using information that the administrator provides through a series of prompts.

The route plan that the external route plan wizard generates includes the following elements:

- Route filters
- Route groups
- Route lists
- Route patterns
- Partitions
- Calling search spaces
- Calling party and calling party transformations
- Access code manipulation

The following topics describe the basic concepts that are used when you generate route plans with the external route plan wizard:

- Generated Route Filters, page 17-34
- Generated Route Groups, page 17-35
- Generated Route Lists, page 17-35
- Generated Route Patterns, page 17-36

Generated Route Filters

A generated route filter permits or restricts access through a route list by using route patterns. The external route plan wizard associates each route list with a particular route filter. It names route filters by using the TenantLocationCalltype convention and appends the suffix RF to each route filter for easy identification.

Table 17-11 shows the seven types of route lists that use route filters. The table shows examples that use specific route filter names and actual access and area codes for better readability.

Table 17-11 Route Lists and Associated Route Filters

Route List Type	Route Filter Name and Content Examples
911 calls	Name: CiscoDallas911RF Content: 9.@ where (SERVICE == 911)
Local calls with metro (7- and 10-digit) dialing	Name: CiscoDallasLocalRF Content: 9.@ where (INTERNATIONAL-ACCESS DOES-NOT-EXIST) AND (LOCAL-AREA-CODE DOES-NOT-EXIST) AND (AREA-CODE DOES-NOT-EXIST) AND (SERVICE DOES-NOT-EXIST) OR (LOCAL-AREA-CODE == 972) OR (LOCAL-AREA-CODE == 214)
Local calls with 10-digit dialing	Name: CiscoDallasLocal10DCallRF Content: 9.@ where (LOCAL-AREA-CODE == 972) OR (LOCAL-AREA-CODE == 214)
Local calls with 7-digit dialing	Name: CiscoDallasLocal7DCallRF Content: 9.@ where (INTERNATIONAL-ACCESS DOES-NOT-EXIST) AND (AREA-CODE DOES-NOT-EXIST) AND (SERVICE DOES-NOT-EXIST)
Toll bypass calls	Name: CiscoTollByPassToDallasRF Content: 9.@ where (AREA-CODE == 972) OR (AREA-CODE == 214)
Long-distance calls	Name: CiscoDallasLongDistanceRF Content: 9.@ where (AREA-CODE EXISTS)
International calls	Name: CiscoDallasIntlRF Content: 9.@ where (INTERNATIONAL-ACCESS EXISTS)

Generated Route Groups

A generated route group sets the order of preference for gateway and port usage. The external route plan wizard assigns one gateway to each generated route group. The wizard uses all ports on the gateways. It does not support using partial resources for generated external route plans.

The external route plan wizard names route filters by using the TenantLocationGatewayTypeNumber convention for easy identification. The following list shows the gateway type abbreviations:

- AA: analog access
- DA: digital access
- HT: H.323 trunk
- MS: MGCP station
- MT: MGCP trunk

The external route plan wizard identifies route groups that are associated with multiple gateways of the same type by attaching a number suffix to all route groups. For example, if three MGCP trunk gateways exist at the Cisco Dallas location, the external route plan wizard names the associated route groups CiscoDallasMT1, CiscoDallasMT2, and CiscoDallasMT3.

If a route list includes more than one route group and more than one gateway (with one gateway for each route group), an arbitrary order designates how the external route plan wizard lists the route groups. The only order that is imposed ensures that route groups that are associated with the local gateways are listed before the route groups that are associated with remote gateways. If needed, manually change the order after the route plan is generated.

Note Cisco Unified CallManager treats all gateways that belong to a location as shared resources for that location.

Generated Route Lists

A generated route list sets the order of preference for route group usage and defines the route filters that are applied to those route groups. The external route plan wizard creates between five and seven route lists for each location depending on the types of local dialing choices that are available. Therefore, the total number of route lists depends on the local dialing scheme and the number of locations that the route plan serves.

Using the TenantLocationCalltype convention, the external route plan wizard names route lists and appends the suffix RL to each route list for easy identification.

Table 17-12 shows the various types of route lists. The examples shown in this table use specific route list names for better readability.

Table 17-12 Route List Types

Route List Type	Example Route List Name and Usage
911 calls	Name: CiscoDallas911RL Use: This route list type applies for 911 emergency calls.
Enterprise calls	Name: CiscoDallasEnterpriseRL Use: This route list type applies for route plans that include Cisco Unified CallManager to adjacent PBX calls. If the route plan does not include routing to an adjacent PBX, the wizard does not generate this route list type.
Local calls with metro dialing	Name: CiscoDallasLocalRL Use: This route list type applies for route plans that encompass both 7- and 10-digit dialing areas. This route list type generates two route lists: one for 7-digit dialing and another for 10-digit dialing. If you chose to generate a route plan that uses metro route lists, you cannot also choose 7- or 10-digit dialing route lists.
Local calls with 10-digit dialing	Name: CiscoDallasLocal10DCallRL Use: This route list type applies for route plans that use 10-digit dialing. This route list type generates one route list for 10-digit dialing. If you chose to generate a route plan that uses a 10-digit dialing route list, you cannot also choose 7-digit or metro dialing route lists.
Local calls with 7-digit dialing	Name: CiscoDallasLocal7DCallRL Use: This route list type applies for route plans that use 7-digit dialing. This route list type generates one route list for 7-digit dialing. If you chose to generate a route plan that uses a 7-digit dialing route list, you cannot also choose 10-digit or metro dialing route lists.
Toll bypass calls	Name: CiscoTollByPassToDallasRL Use: This route list type applies for intracluster calls that originate from a remote location and that get routed out the local gateway as local calls.
Long-distance calls	Name: CiscoDallasLongDistanceRL Use: This route list type applies for long-distance toll calls.
International calls	Name: CiscoDallasIntlRL Use: This route list type applies for international toll calls.

Generated Route Patterns

A generated route pattern directs calls to specific devices and either includes or excludes specific dialed-digit strings. The external route plan wizard only generates route patterns that require an access code prefix. The typical route pattern for routing a call to the PSTN includes the prefix construction 9.@. The typical route pattern for routing a call to the PBX includes the prefix construction 9.9@.

The external route plan wizard associates a route list, a route filter, and a partition with each route pattern. The route pattern provides the appropriate calling party transform mask, called party transform mask, discard digits instructions, and prefix digits for the associated route list.

The wizard bases route patterns for calls to an adjacent PBX on the access code and the range of directory numbers that are served by that PBX. For example, if the access code that is used to direct calls to the adjacent PBX is 9 and the range of directory numbers that is served by that PBX is 1000 through 1999, the external route plan wizard generates the route pattern 9.1XXX for enterprise calls.

Route Plan Report

The route plan report comprises a listing of all unassigned directory numbers (DN), call park numbers, call pickup numbers, conference numbers (Meet-Me numbers), directory numbers, route patterns, translation patterns, voice-mail ports, message-waiting indicators, and attendant console numbers in the system.

The route plan report allows you to view either a partial or full list and to go directly to the associated configuration windows by choosing a route pattern, partition, route group, route list, directory number, call park number, call pickup number, conference number (Meet-Me number), or gateway.

Using the route plan report, you can get a list of unassigned directory numbers and delete those numbers from the Cisco Unified CallManager database, if required.

In addition, the route plan report allows you to save report data into a .csv file that you can import into other applications such as the Bulk Administration Tool (BAT). The .csv file contains more detailed information, including directory numbers (DN) for phones, route patterns, and translation patterns. Refer to the "Route Plan Report" section in the *Cisco Unified CallManager Administration Guide* for more information.

Where to Find More Information

Related Topic

- Partitions and Calling Search Spaces, page 15-1

Related Cisco Documentation

- Partition Configuration, *Cisco Unified CallManager Administration Guide*
- Calling Search Space Configuration, *Cisco Unified CallManager Administration Guide*
- Route Group Configuration, *Cisco Unified CallManager Administration Guide*
- Route List Configuration, *Cisco Unified CallManager Administration Guide*
- Route Pattern Configuration, *Cisco Unified CallManager Administration Guide*
- Line Group Configuration, *Cisco Unified CallManager Administration Guide*
- Hunt List Configuration, *Cisco Unified CallManager Administration Guide*
- Hunt Pilot Configuration, *Cisco Unified CallManager Administration Guide*
- Presence, *Cisco Unified CallManager Features and Services Guide*
- *Cisco Unified Communications Solution Reference Network Design (SRND)*

CHAPTER 18

Understanding Directory Numbers

Using the Directory Number Configuration window in Cisco Unified CallManager Administration, you can configure and modify directory numbers (lines) that are assigned to phones. Keep in mind, however, that directory numbers (DNs) do not always associate with devices (see the "Managing Directory Numbers" section on page 18-5).

This section covers the following topics:

- Characteristics of Directory Numbers, page 18-1
- Shared Line Appearance, page 18-2
- Managing Directory Numbers, page 18-5
- Directory Number Features, page 18-5
- Making and Receiving Multiple Calls Per Directory Number, page 18-7
- Directory Number Search, page 18-8
- Dependency Records, page 18-9
- Directory Number Configuration Checklist, page 18-9
- Where to Find More Information, page 18-10

Characteristics of Directory Numbers

You can configure up to 200 calls for a line on a device in a cluster, with the limiting factor being the device. As you configure the number of calls for one line, the calls that are available for another line decrease. Cisco Unified IP Phones that support the multicall display (such as a Cisco Unified IP Phone model 7960) support up to 200 calls per DN and 2 calls per DN for non-multicall display devices (such as Cisco Unified IP Phone model 7905).

The Cisco Unified IP Phone displays the following information about each line:

- Unique call identifier (from 1 to 200). This identifier remains consistent across all multicall display devices that have a shared-line appearance.
- Call select status, an icon that shows the state of the currently selected call
- Call information such as calling party or called party
- Call state icon such as connected or hold
- Duration of a call

For configuration information, refer to the "Configuring a Directory Number" section in the *Cisco Unified CallManager Administration Guide*.

User/Phone Add and Directory Numbers

The End User, Phone, DN, and LA Configuration window allows all-at-once addition of a new end user and a new phone that is associated with the new end user. You can associate a directory number (existing or new) and line appearance for the new end user by using the same window. To access the End User, Phone, DN, and LA Configuration window, choose the **User Management > User/Phone Add** menu option. See "User/Phone Add Configuration" in the *Cisco Unified CallManager Administration Guide* for configuration details.

Note The End User, Phone, DN, and LA Configuration window only allows addition of a new end user and a new phone. The window does not allow entry of existing end users or existing phones.

Shared Line Appearance

You can set up one or more lines with a shared-line appearance. A Cisco Unified CallManager system considers a directory number to be a shared line if it appears on more than one device in the same partition. For example, if directory number 9600 on phone A is in the partition called Dallas and on phone B in the partition called Texas, that directory number does not represent a shared-line appearance. (Ensure the directory number 9600 for phone A and phone B are in the same partition; for example, Dallas.)

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. Another example of a shared line involves a single incoming 800 number that is set up to appear as line 2 on every sales representative phone in an office. You can also choose to update a directory number and have the updates apply to all devices that share the directory number.

The following information provides tips about and lists the restrictions for using shared-line appearances with Cisco Unified CallManager.

Shared Line Tips

Use the following tips when configuring shared lines:

- You create a shared-line appearance by assigning the same directory number and route partition to different devices.
- If multiple devices share a line, each device name displays in the Associated Devices pane of the directory number in the Directory Number Configuration window in Cisco Unified CallManager Administration.
- If you change the Calling Search Space or Call Forward and Pickup settings on any device that uses the shared line, the changes apply to all devices that use that shared line.
- To stop sharing a line appearance on a device, change the directory number or partition name for the line and update the directory number in the Directory Number Configuration window in Cisco Unified CallManager Administration.
- In the case of a shared-line appearance, Remove From Device removes the directory number on the current device only and does not affect other devices.

- Most devices with a shared-line appearance can make or receive new calls or resume held calls at the same time. Incoming calls display on all devices that share a line, and anyone can answer the call. Only one call remains active at a time on a device. For limitations, see the "Shared Line Restrictions" section on page 18-4.

Note Cisco SIP IP Phones models 7905, 7912, 7940, and 7960 will not display remote-in-use calls and cannot do remote resume (cannot pick up a held line that is shared). These Cisco SIP phones do not support shared-line features such as Barge, cBarge, and Privacy.

- Call information (such as calling party or called party) displays on all devices that are sharing a line. If one of the devices turns on the Privacy feature, other devices that share the line will not see outbound calls that are made from the device that turned on privacy. All devices will still see inbound calls to the shared line.
- Devices with shared-line appearances can initiate independent transfer transactions.
- Devices with shared-line appearances can initiate independent conference transactions.
- Devices with shared-line appearance support the Call Forward Busy Trigger and the Maximum Number of Calls settings. You can configure Call Forward Busy Trigger per line appearance, but the configuration cannot exceed the maximum number call setting for that directory number.

  The following example demonstrates how three Cisco Unified IP Phones with the same shared-line appearance, directory number 2000, use Call Forward Busy Trigger and Maximum Number of Calls settings. This example assumes that two calls occur. The following values configuration applies for the devices:

  - Cisco Unified IP Phone 1—Configured for a maximum call value of 1 and busy trigger value of 1
  - Cisco Unified IP Phone 2—Configured for a maximum call value of 1 and busy trigger value of 1
  - Cisco Unified IP Phone 3—Configured a for maximum call value of 2 and busy trigger value of 2

  When Cisco Unified IP Phone User 1 dials directory number 2000 for the first call, all three devices ring. The user for the Cisco Unified IP Phone 3 picks up the call, and the Cisco Unified IP Phones 1 and 2 go to remote in use. When the user for Cisco Unified IP Phone 3 puts the call on hold, user can retrieve the call from the Cisco Unified IP Phone 1 or Cisco Unified IP Phone 2. When User 2 dials directory number 2000 for the second call, only Cisco Unified IP Phone 2 and Cisco Unified IP Phone 3 ring.

  The following example demonstrates how an H.323 client, MGCP POTS phone, and Cisco Unified IP Phone with the same shared line appearance, directory number 2000, can use the Call Forward Busy Trigger and the Maximum Number of Calls settings. This example assumes that two calls occur. The following values configuration applies for the devices:

  - H.323 client—Configured for a maximum call value of 1 and busy trigger value of 1
  - MGCP POTS Phone—Configured for a maximum call value of 1 and busy trigger value of 1
  - Cisco Unified IP Phone—Configured for a maximum call value of 2 and busy trigger value of 2

  When User 1 dials directory number 2000 for the first call, all three devices ring. The user for the Cisco Unified IP Phone picks up the call; when the user for Cisco Unified IP Phone puts the call on hold, the user(s) for H323 client and MGCP POTS phone cannot retrieve the call. If User 2 dials directory number 2000 for the second call, all three devices (IP phone, MCGP POTS phone, H.323 client) ring, and all three users can answer the call.

For information on Maximum Number of Calls setting, refer to the "Directory Number Configuration Settings" section in the *Cisco Unified CallManager Administration Guide*.

The check box, Update Directory Number of All Devices Sharing this Line, in the Directory Number Configuration window, determines whether a shared directory number gets updated to all devices that share the number. See the "Update Directory Number of All Devices Sharing This Line" section on page 18-5 for more information.

A shared-line phone should not be able to interact with the call that it rejects, due to the limitation of the maximum number of calls per DN or for other reasons. For example, A and A^1 share the same DN. A^1 and A have the maximum number of calls set to 1 and 2, respectively. When C and D call the share line DN, A^1 answers these two calls. A can only interact with the first call, as it rejects the second call due to its own maximum number of calls per DN limitation. For this reason, Cisco recommends that the same value be configured for the maximum number of calls for all shared-line MCID devices. For N number of devices that share the same line, ensure both Maximum Calls setting and Busy Trigger setting are set to N. This allows each shared-line user to receive at least one call.

The shared-line phone should not interact with the call that it does not receive (because the Line Control does not maintain call information). So, a newly registered device will not recognize any existing calls on that line. The newly registered device cannot resume any held call if the call started before this device was registered with the Line Control. For example, A and A^1 share the same line, A is powered down (or logged out for the extension mobility user), and A's receives an active call. After phone A is on and it registers with Cisco Unified CallManager, A should not see the existing active call in this line.

If shared-line phones' calls should interact with each other, Cisco recommends that you set the maximum number of calls for all shared-lines MCID devices to 2*N, where N specifies the number of shared-line devices.

Shared Line Restrictions

The following restrictions apply to shared lines:

- Do not use shared lines for Cisco Unified CallManager Attendant Console pilot points or hunt group members. The phone that acts as the attendant console supports shared lines.
- Do not use shared-line appearances on any Cisco Unified IP Phone that requires autoanswer capability and do not turn on auto answer for a shared-line appearance.
- Do not configure shared-line appearances on the primary lines of the phones; for example, if two phones have a shared-line appearance, only one of the phones should have the primary line configured as shared (the other phone should have the secondary line configured as shared).
- Barge and Privacy work with shared lines only.
- Cisco recommends that you do not configure shared lines for Cisco Unified IP Phones, H.323 clients, and MGCP POTS phones; likewise, Cisco recommends that you do not configure shared lines for H.323 clients and MGCP POTS phones. If you configure the same shared-line appearance for a H.323 client, a MGCP POTS phone, for example, NetMeeting, and a Cisco Unified IP Phone, you cannot use the hold/resume feature on the H.323 client or MGCP POTS phone.
- Cisco recommends that you do not configure shared lines for Cisco SIP IP Phone models 7905, 7912, 7940, and 7960 because these phones cannot pick up held calls on shared lines nor can they use the shared-line features Barge, cBarge, and Privacy.

Managing Directory Numbers

Directory numbers associate with devices such as phones, route points, CTI ports, and H.323 clients. Administrators manage directory numbers from the Directory Number Configuration and Route Plan Report windows in Cisco Unified CallManager Administration. Use the Directory Number Configuration window or the Phone Configuration window to add, update, and remove directory numbers from a device, route point, or port. Use the Route Plan Report window to delete or update unassigned directory numbers from Cisco Unified CallManager database.

Note Do not associate a directory number with a CTI route point or CTI port if the directory number is a member of a line group.

The Directory Number Configuration window contains two check boxes: Active and Update Directory Number of All Device Sharing this Line.

Active Check Box

The Active check box, which only displays for unassigned directory numbers, determines whether the directory number gets loaded and used by Cisco Unified CallManager. By checking the check box, the directory number gets loaded and used by Cisco Unified CallManager. For example, the directory number belonged to an employee who left the company. The directory number had certain settings that were configured, such as call forwarding to voice messaging. By leaving the directory number active, a call that is intended for the directory number will get forwarded. This eliminates the need to reconfigure another employee to have the same call-forwarding options. If the check box is not checked, the directory number will not get loaded by Cisco Unified CallManager, which results in settings that are configured for that DN to not be used (for example, call forward destinations), and callers will not get their call forwarded properly.

Update Directory Number of All Devices Sharing This Line

This check box determines whether a shared directory number gets updated to all devices that share the number. When the check box is checked, all devices that share the directory number will receive the directory number change. If the check box remains unchecked, only the current device that is displayed in the window gets the directory number changed, and all other devices that share the directory number remain unchanged.

Note This check box only applies to the actual directory number and partition. It does not apply to the other device settings such as voice-messaging profile, call forwarding options, or MLPP. If any of these settings are changed for a shared line, all devices get changed.

For directory number configuration and update information, refer to the "Directory Number Configuration Overview" section in the *Cisco Unified CallManager Administration Guide*. For information about deleting and updating unassigned directory numbers, refer to "Deleting Unassigned Directory Numbers" and "Updating Unassigned Directory Numbers" in the *Cisco Unified CallManager Administration Guide*.

Directory Number Features

Cisco Unified CallManager enables you to configure the following features for directory numbers: call waiting and call forward.

For information about features that relate to phones, see the "Phone Features" section on page 43-20. The following features get configured for phones: barge, privacy release, call back, call park, call pickup, immediate divert, malicious call identification, quality report tool, service URL, and speed dial and abbreviated dial

Call Forward

Call forward allows a user to configure a Cisco Unified IP Phone, so all calls that are destined for it ring another phone. The following types of call forward exist:

- Call forward all—Forwards all calls.
- Call forward busy—Forwards calls only when the line is in use and busy trigger setting is reached.
- Call forward no answer—Forwards calls when the phone is not answered after the configured no answer ring duration, or if the destination is unregistered.
- Call forward no coverage—Forward calls when either exhausts or times out, and the associated hunt-pilot for coverage specifies Use Personal Preferences for its final forwarding.

You can configure each of these call forward types for internal and external calls that can be forwarded to voice messaging system, dialed destination number, or calling search space.

Cisco Unified CallManager release 5.0 supports a secondary Calling Search Space (CSS) for Call Forward All (CFA) field. The secondary CSS for CFA combines with the existing CSS for CFA to allow the support of the alternate CSS system configuration. When CFA is activated, only the primary and secondary CSS for CFA get used to validate the CFA destination and redirect the call to the CFA destination. If these fields are empty, the null CSS gets used. The combination of the line CSS and device CSS no longer gets used when the CSS for CFA is None. Only the CSS fields that are configured in the primary CSS for CFA and secondary CSS for CFA fields get used. If CFA is activated from the phone, the CFA destination gets validated by using the CSS for CFA and the secondary CSS for CFA and the CFA destination gets written to the database. In previous releases, if the CSS for CFA is empty, the CFA destination got validated against the combination of the line CSS and device CSS of the phone. In this release, when the CFA is activated, the CFA destination always gets validated against the CSS for CFA and the secondary CSS for CFA.

The administrator can configure call forward information display options to the original dialed number or the redirected dialed number or both. The administrator can enable or disable the calling line ID (CLID) and calling name ID (CNID). The display option gets configured for each line appearance.

The call forward busy trigger gets configured for each line appearance in a cluster and cannot exceed the maximum number of calls that are configured for a line appearance. The call forward busy trigger determines how many active calls exist on a line before the call forward busy setting gets activated (for example, 10 calls).

The call forward no answer ring duration gets configured for each line appearance in a cluster, and the default specifies 12 seconds. The call forward no answer ring duration determines how long a phone rings before the call forward no answer setting gets activated.

Tip Keep the busy trigger slightly lower than the maximum number of calls, so users can make outgoing calls and perform transfers.

Configure call forward in the Directory Number Configuration window in Cisco Unified CallManager Administration.

Call Waiting

Call waiting lets users receive a second incoming call on the same line without disconnecting the first call. When the second call arrives, the user receives a brief call-waiting indicator tone, which is configured with the Ring Setting (Phone Active) in the Directory Number Configuration window.

Configure call waiting in the Directory Number Configuration window in Cisco Unified CallManager Administration by setting the busy trigger (greater than 2) and maximum number of calls.

Tip To configure call waiting for phones with no display (such as the Cisco IP Phone model 30 VIP), set the busy trigger to 2 and the maximum number of calls to 2.

Making and Receiving Multiple Calls Per Directory Number

Cisco Unified CallManager supports various behaviors when users make and receive multiple calls per DN: Transfer/Direct Transfer and Conference/Join.

Transfer allows different line appearances in one device to initiate independent transfer transactions and allows multiple transfer transactions per line appearance per device.

Conference allows different line appearances in one device to initiate independent conference transactions and allows multiple conference transactions per line appearance per device.

Note Devices that do not support multicall display, such as Cisco Unified IP Phone model 7910, cannot transfer or conference two existing calls together.

Transfer and Conference Behavior

If only one active call exists on the directory number, the first invocation of a feature results in putting the active call on hold and initiating a new call by using the same directory number. When the new call gets set up, the second invocation of the same feature starts the feature operation. The first invocation of Transfer/Conference will always initiate a new call by using the same directory number, after putting the active call on hold.

Direct Transfer and Join Behavior

The following information describes Direct Transfer and Join behavior:

- Direct Transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Direct Transfer does not initiate a consultation call and does not put the active call on hold.
- Join does not create a consultation call and does not put the active call on hold. To implement Join, choose at least two calls and then press the Join softkey on one of the calls. Join can include more than two calls, which results in a call with three or more parties. Join supports up to 16 participants in a call. To choose an active or held call, highlight the call and press the Select softkey. A checked indicator displays next to a selected call on the phone.

The call that initiates the Join automatically gets included, even if it is not selected. The active call gets included even if not selected. If all the calls in the join represent a basic call, the call that initiated the join represents the primary call. If any call in the join is a conference call (that is, it was in a conference before being joined), that call represents the primary call.

The selected status of the final call after the join depends on the selected status of the primary call before the join. If the primary call was selected, the final call remains selected after the join. This means that if that call is put on hold, shared lines would not be able to retrieve the call because the call is still selected. If the primary call was not selected, the final call remains unselected after the call.

Note If more than one call in the join is a conference call, the join will fail (join supports only one conference call).

Directory Number Search

The following sections describe how to modify your search to locate a directory number. If you have thousands of directory numbers in your network, you may need to limit your search to find the directory number that you want. If you cannot locate a directory number, you may need to expand your search to include more directory numbers.

Note Be aware that the directory number search is not case sensitive.

Searching by Directory Number

To search for a phone by its directory number (DN), choose Directory Number and either enter a search criteria (such as begins with or ends with) or click the **Find** button.

Note Some directory numbers do not associate with phones. To search for those directory numbers, which are called unassigned DN, use the Route Plan Report window.

Searching by Route Partition

To search for a phone by its route partition, choose Route Partition and either enter a search criteria (such as begins with or ends with) or click the **Find** button.

Searching by Description

To search for a phone by its description, choose Description and either enter a search criteria (such as begins with or ends with) or click the **Find** button.

Search Within Results

To refine your search results, you can search for additional information. For example, if you search for directory numbers by directory number, you may want to search within the directory number results for DNs that share the same route partition. After you perform an initial search, check the Search Within Results check box. You can enter additional, or different, search criteria in the drop-down list boxes. Click **Find** again to search within the previous results.

Finding All Directory Numbers in the Database

To find all directory numbers that are registered in the database, choose Directory Number from the list of fields; choose "is not empty" from the list of patterns; then, click the **Find** button.

Dependency Records

If you need to find out the directory numbers that a specific phone is using or the phones to which a directory number is assigned, choose Dependency Records from the Related Links drop-down list box on the Cisco Unified CallManager Administration Phone Configuration or Directory Number Configuration window. The Dependency Records Summary window displays information about directory numbers that are using the phone. To find out more information about the directory number, click the directory number 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 the "Accessing Dependency Records" section and the "Removing a Directory Number from a Phone" section in the *Cisco Unified CallManager Administration Guide*.

Directory Number Configuration Checklist

Table 18-1 provides steps to manually configure a directory number in Cisco Unified CallManager Administration. If you are using autoregistration, Cisco Unified CallManager adds the phone and automatically assigns the directory number.

Table 18-1 Directory Number Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	If you want to configure a DN for a phone, add and configure the phone. You may need the following information about the phone: • Model • MAC address • Physical location of the phone • Cisco Unified CallManager user to associate with the phone • Partition, calling search space, and location information, if used • Number of lines and associated DNs to assign to the phone	Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 2	Add and configure lines (DNs). Configure DNs either from the Directory Number Configuration window or, if you want to configure a DN for a phone, from the Phone Configuration window. You can also configure phone features such as call park, call forward, and call pickup.	Configuring a Directory Number, *Cisco Unified CallManager Administration Guide* Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*

Table 18-1 Directory Number Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 3	Configure speed-dial buttons. You can configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the speed-dial settings on their phones by using Cisco IP Phone User Options.	Configuring Speed-Dial Buttons, *Cisco Unified CallManager Administration Guide*
Step 4	Configure Cisco Unified IP Phone services. You can configure services for Cisco Unified IP Phone models 7970, 7960, 7940, 7912, and 7905 and Cisco IP Communicator if you want to provide services for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the services on their phones by using the Cisco IP Phone User Options.	Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 5	Customize phone button templates and softkey templates, if required. Configure templates for each phone.	Configuring Phone Button Templates, *Cisco Unified CallManager Administration Guide* Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide* Adding Nonstandard Softkey Templates, *Cisco Unified CallManager Administration Guide*
Step 6	Assign services to phone buttons, if required.	Adding a Cisco Unified IP Phone Service to a Phone Button, *Cisco Unified CallManager Administration Guide*
Step 7	Provide power, install, verify network connectivity, and configure network settings for the Cisco Unified IP Phone.	*Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*
Step 8	Associate a user with the phone (if required).	Associating Devices to an End User, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topics

- Cisco Unified IP Phones, page 43-1
- Voice Mail Connectivity to Cisco Unified CallManager, page 29-1
- Call Pickup Group, page 34-1
- Directory Number Configuration, *Cisco Unified CallManager Administration Guide*
- Enabling Autoregistration, *Cisco Unified CallManager Administration Guide*
- Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
- Associating Devices to an End User, *Cisco Unified CallManager Administration Guide*

- User/Phone Add Configuration, *Cisco Unified CallManager Administration Guide*
- Phone Button Template Configuration, *Cisco Unified CallManager Administration Guide*
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
- Barge and Privacy, *Cisco Unified CallManager Features and Services Guide*
- Call Park, *Cisco Unified CallManager Features and Services Guide*
- Immediate Divert, *Cisco Unified CallManager Features and Services Guide*
- Quality Report Tool, *Cisco Unified CallManager Features and Services Guide*

Additional Cisco Unified CallManager Documentation

- Phone administration documentation that supports your phone model and this version of Cisco Unified CallManager
- Cisco Unified IP Phone user documentation, including Getting Started documents
- Firmware release notes for your phone model
- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Security Guide*
- *Cisco Unified CallManager Assistant User Guide*
- *Cisco IP Communicator Administration Guide*

CHAPTER 19

Dial Rules Overview

Cisco Unified CallManager supports different types of dial rules: Application Dial Rules, Directory Lookup Dial Rules, and SIP Dial Rules.

The administrator uses Application Dial Rules to add and sort the priority of dialing rules for applications such as Cisco WebDialer, Cisco Unified CallManager Assistant, and Cisco Unified CallManager Attendant Console. Application Dial Rules automatically strip numbers from or add numbers to telephone numbers that the user dials. For example, the dial rules automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

In Cisco Unified CallManager Assistant, the assistant can perform a directory search from the assistant console. The assistant can drag and drop the directory entry to the My Calls panel on the assistant console, which invokes a call to the number that is listed in the entry. The dial rules apply to the number that is listed in the entry before the call gets made.

Cisco Unified CallManager Attendant Console uses directory lookup rules to transform caller identification numbers into numbers that can be looked up in the directory. If Cisco Unified 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.

Cisco Unified CallManager performs system digit analysis and routing; however, the Cisco SIP IP Phone needs to know when enough digits are collected before call processing takes place, so the administrator configures SIP Dial Rules and adds the SIP dial rule to the phone.

The following sections describe dial rules:

- Application Dial Rules Configuration Design, page 19-1
- Application Dial Rules Configuration Error Checking, page 19-2
- Directory Lookup Dial Rules, page 19-3
- SIP Dial Rules, page 19-4
- Where to Find More Information, page 19-8

Application Dial Rules Configuration Design

The Application Dial Rules Configuration window organization includes the following information:

- Name—This field comprises a unique name for the dial rule that can contain up to 20 alphanumeric characters and any combination of spaces, periods (.), hyphens (-), and underscore characters (_).
- Description—This field comprises a brief description that you enter for the dial rule.

- Number Begins With—This field comprises the initial digits of the directory numbers to which you want to apply this application dial rule.
- Number of Digits—This required field comprises the initial digits of the directory numbers to which you want to apply this application dial rule.
- Total Digits to be Removed—This required field comprises the number of digits that you want Cisco Unified CallManager to remove from directory numbers that apply to this dial rule.
- Prefix With Pattern—This required field comprises the pattern to prepend to directory numbers that apply to this application dial rule.
- Application Dial Rule Priority—This field, that displays when you enter the Prefix With Pattern information, allows you to set the priority order of the application dial rules.

The following example provides a dial rule condition and the consequence when a dial rule is created.

Condition

- If the phone number begins with (the field is *blank*)—This condition leaves blank one or more digits at the beginning of the number that the user dialed. For example, if the user dialed 1, 1500, or 1500555, each would match the dial number 15005556262.
- and the number of digits is (the field is *blank*)—This condition leaves blank the total number of digits in the telephone number that the user dialed. For example, if the dial number is 915005556262, the number of digits equals 12.

Consequence

- Remove *blank* digits from the beginning—The application deletes this number of digits from the front of the dialed number. For example, if 4 is specified, and the dialed number is 15005556262, the application removes 1500, leaving 5556262.
- and prefix it with (this field is *blank*)—After removing the specified number of digits, the application adds this string of numbers to the front of the dialed number. For example, if 9 was specified, the application adds 9 to the front of the dialed number (could be specifying an outside line).

Application Dial Rules Configuration Error Checking

The application dial rules perform the following error checking in the Dial Rule Creation section of the Dial Rules Configuration window:

- The phone number begins with field supports only digits and the characters +*#. The length cannot exceed 100 characters.
- The number of digits is field supports only digits, and the value in this field cannot be less than the length of the pattern that is specified in the pattern field. This field cannot be blank for a dial rule.
- The remove digits field supports only digits, and the value in this field cannot be more than the value in the number of digits is field.
- The prefix it with field supports only digits and the characters +*#. The length cannot exceed 100 characters.
- Ensure that dial rules are unique.
- The remove digits field and the prefix it with field cannot both be blank for a dial rule.

Directory Lookup Dial Rules

Cisco Unified CallManager Attendant Console uses directory lookup rules to transform caller identification numbers into numbers that can be looked up in the directory. If Cisco Unified 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.

The Directory Lookup Dial Rules window allows you to enter the following information for each dial rule:

- Name—This field comprises a unique name for the dial rule that can contain up to 20 alphanumeric characters and any combination of spaces, periods (.), hyphens (-), and underscore characters (_).
- Description—This field comprises a brief description that you enter for the dial rule.
- Number Begins With—This field comprises the initial digits of the directory numbers to which you want to apply this application dial rule.
- Number of Digits—This required field comprises the length of the directory numbers to which you want to apply this directory lookup dial rule.
- Total Digits to be Removed—This required field comprises the number of digits that you want Cisco Unified CallManager to remove from directory numbers that apply to this dial rule.
- Prefix With Pattern—This required field comprises the pattern to prepend to directory numbers that apply to this dial rule.

Directory Lookup Dial Rule Example

You can create a directory lookup rule that automatically adds 40852 to 5-digit numbers beginning with 5. Using this rule, the number 56666 becomes 4085256666. If 408525666 matches a user in the speed-dial entries on the attendant PC or in the directory, Cisco Unified CallManager displays the name in the Call Details window.

To create this rule, enter the following information on the Directory Lookup Dial Rules window:

- In the Number Begins With field, enter “5,” so the dial rule applies to numbers that begin with the number 5.
- In the Number of Digits field, enter the number of digits “5,” so the dial rule applies to numbers that contain 5 digits.
- In the Prefix With Pattern field, enter “40852,” so the dial rules prepends 40852 to numbers that apply to this dial rule.

Limitations

When creating a directory lookup rule, consider the following limitations:

- The phone number begins with field supports only digits and the characters +*#. The length cannot exceed 100 characters.
- The number of digits is field supports only digits, and the value in this field cannot be less than the length of the pattern that is specified in the pattern field.
- The remove digits field supports only digits, and the value in this field cannot be more than the value in the number of digits is field.
- The prefix it with field supports only digits and the characters +*#. The length cannot exceed 100 characters.
- The remove digits field and the prefix it with field cannot both be blank for a dial rule.

For information on working with directory lookup rules, see the "Directory Lookup Dial Rules Configuration" section in the *Cisco Unified CallManager Administration Guide*.

SIP Dial Rules

The administrator uses SIP dial rule configuration to configure SIP phone dial plans and associate them with the following SIP phones:

- Cisco SIP IP Phone model 7911, 7941, 7961, 7970, and 7971. These phones use the 7940_7960_OTHER dial rules patterns. Key Press Markup Language (KPML) allows for the digits to be sent to Cisco Unified CallManager digit by digit; SIP Dial Rules allow for a pattern of digits to be collected locally on the phone prior to sending to Cisco Unified CallManager. If SIP dial rules are not configured, KPML gets used. To increase the performance of Cisco Unified CallManager (increasing the number of calls that get processed), Cisco recommends that administrators configure SIP dial rules.
- Cisco SIP IP Phone model 7940 and 7960. These phones use the 7940_7960_OTHER dial rules pattern and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must wait a specified time before digits are sent to Cisco Unified CallManager for processing. This delays the actual call from being processed.
- Cisco SIP IP Phone model 7905 and 7912. These phones use the 7905_7912 dial rules pattern and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must wait a specified time before digits are sent to Cisco Unified CallManager for processing. This delays the actual call from being processed.

Although SIP dial rules are optional, if they are configured, you must add them to the SIP phone by using the Phone Configuration window of Cisco Unified CallManager Administration. (If the administrator configures SIP dial plans, those dial plans must get associated with a SIP phone device, so the dial plans get sent to the device configuration file.) Leave the SIP Dial Rules field in the Phone Configuration window set to <None> if you do not want dial rules applied to the Cisco SIP IP Phone.

After the administrator configures the SIP dial rule and applies it to the SIP phone by pressing Reset, the database sends the TFTP server a notification, so it can build a new set of configuration files for the SIP phone. The TFTP server notifies Cisco Unified CallManager about the new configuration file, and the updated configuration file gets sent to the phone. See the "TFTP Process Overview for Cisco SIP IP Phones" section on page 10-3 for more information.

To accommodate extension mobility users, so they can use SIP dial rules, the administrator must configure the SIP dial rule on the phone that will allow extension mobility users to log on.

Note Extension mobility supports Cisco SIP IP Phone model 7941, 7961, 7970, and 7971.

SRST does not support KPML; however, the SIP phone will continue to use the Dial Rules it received from Cisco Unified CallManager when it is in SRST mode.

Administrators use the SIP Dial Rules Configuration window to configure dial rule patterns and the parameters for the pattern.

SIP Dial Rule Patterns

Two types of dial rule patterns exist in the SIP Dial Rules Configuration window:

- 7905_7912—Use this dial rule pattern for Cisco SIP IP Phone model 7905 and 7912.

- 7940_7960_OTHER—Use this dial rule pattern for Cisco SIP IP Phone model 7911, 7940, 7941, 7960, 7961, 7970, and 7971.

After the appropriate dial rule pattern gets chosen, the administrator configures the dial rule parameters for the dial rule pattern.

SIP Dial Rule Parameters

After the administrator defines the dial pattern, the SIP Dial Rule Information window displays, so the administrator can configure the dial pattern parameters such as timeouts, buttons, or Private Line Automatic Ringdown (PLAR).

Ensure all pattern information has a name; for example, PLAR1 or 911. After you name the pattern information, you need to configure the parameters for the pattern. The SIP Dial Rules Configuration window displays an area for the pattern information. The administrator chooses the type of pattern parameter from a drop-down list box that displays on the configuration window. See SIP Dial Rule Configuration Settings, page 30-4, for a description of the dial parameters.

These dial patterns get sent to the TFTP server, which creates the proper configuration file that contains the dial pattern information.

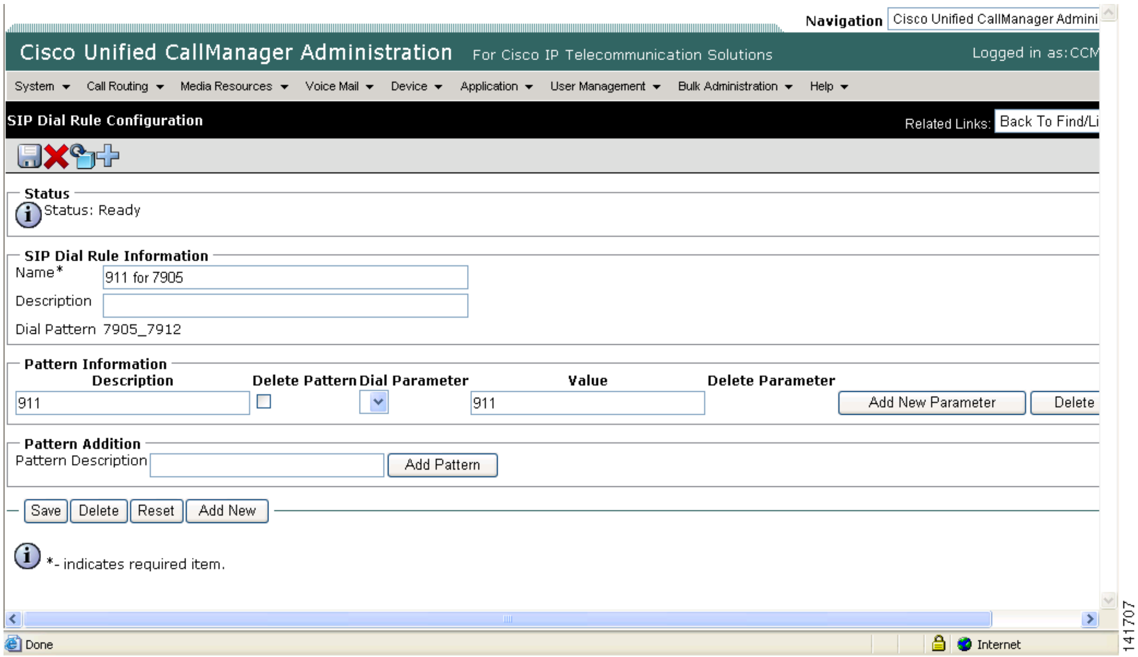
The following examples illustrate how to configure a dial rule for 911 and a pattern for any 4-digit extension beginning with the digit 2.

Sample Dial Rule for 911 on Cisco Unified IP Phone 7905

The administrator wants a dial rule pattern for 911on the Cisco SIP IP Phone model 7905. To accomplish this pattern, the administrator performs the following (see Figure 19-1) steps:

1. Create a 7905_7912 SIP dial rule.
2. Create a pattern called 911 for 7905.
3. Enter a pattern description called 911.
4. In the dial parameter value field, enter 911.

Figure 19-1 05_12 911 Dial Rule Pattern



SIP Dial Rule Configuration

Status

Status: Ready

SIP Dial Rule Information

Name* 911 for 7905

Description

Dial Pattern 7905_7912

Pattern Information

Description	Delete Pattern	Dial Parameter	Value	Delete Parameter
911	□		911	

Pattern Addition

Pattern Description

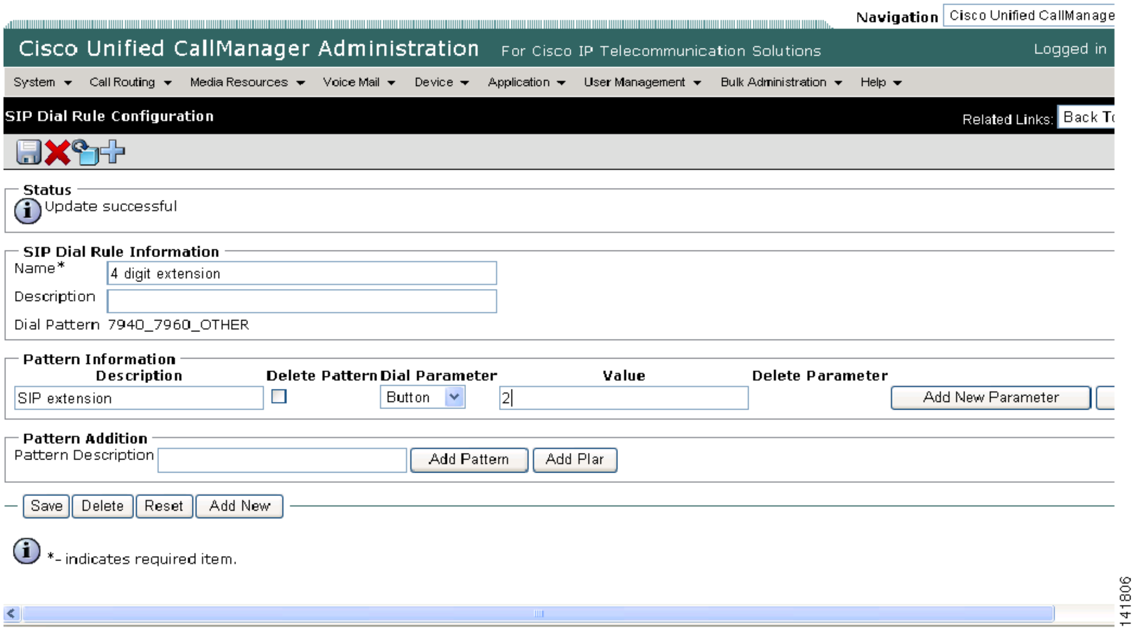
*- indicates required item.

Sample Dial Rule for Extension

The administrator wants a dial rule pattern for any 4-digit extension beginning with the digit 2 on a Cisco SIP IP Phone model 7961. To accomplish this pattern, the administrator performs the following (see Figure 19-2) steps:

1. Create a 7940_7960_OTHER SIP dial rule.
2. Create a pattern called 4-digit extension.
3. Enter a pattern description called SIP extension.
4. In the dial parameter value field, enter 2 followed by three dots (2...).

Figure 19-2 7940_7960_OTHER Dial Rule Pattern



SIP Dial Rule Configuration

Status
Update successful

SIP Dial Rule Information
Name* 4 digit extension
Description
Dial Pattern 7940_7960_OTHER

Pattern Information

Description	Delete Pattern	Dial Parameter	Value	Delete Parameter
SIP extension	□	Button	2	

Pattern Addition
Pattern Description

*- indicates required item.

Private Line Automatic Ringdown (PLAR)

Configure a SIP phone for Private Line Automatic Ringdown (PLAR), so when the user goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a preconfigured number. The phone user cannot dial any other number from the phone line that gets configured for PLAR. Because PLAR gets configured in Cisco Unified CallManager Administration as an empty pattern, it does not get associated with a device or line. To make the SIP IP phone support PLAR, an empty pattern gets configured in the SIP Dial Rules for a specific line, and the dial rule then gets applied to the Cisco SIP IP Phone by using Phone Configuration in Cisco Unified CallManager Administration.

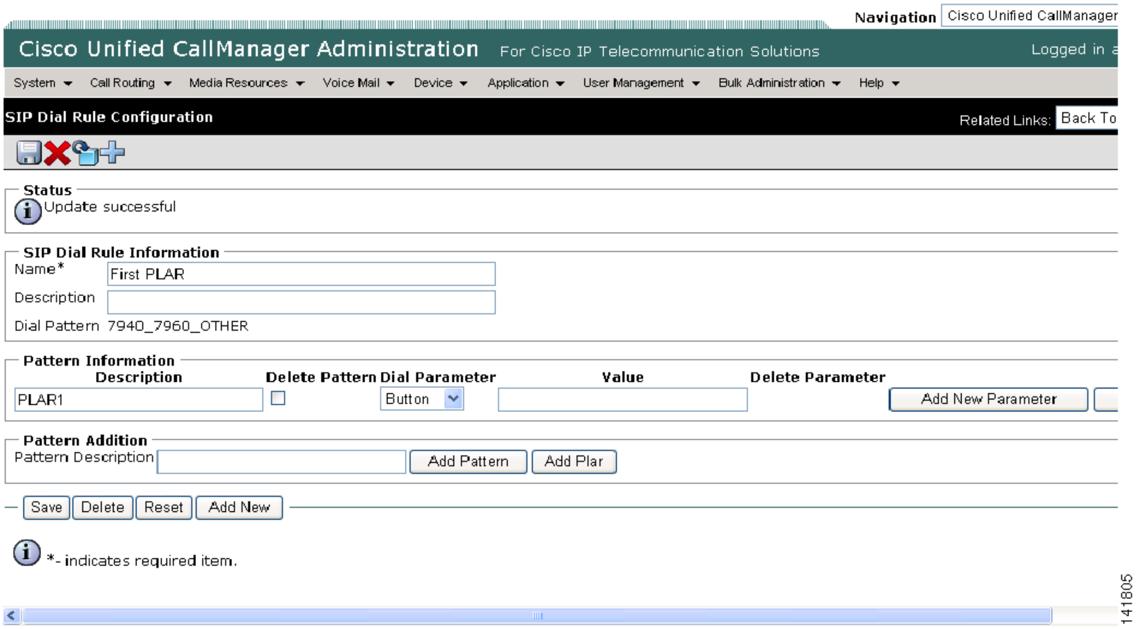
Note Only Cisco SIP IP Phone model 7940/41, 7960/61, and 7970/71 support PLAR.

7940_7960_OTHER Dial Rule Plan for PLAR

The administrator wants a dial rule pattern for PLAR on line 1 of the Cisco SIP IP Phone model 7960. To accomplish this pattern, the administrator performs the following (see Figure 19-3) steps:

1. Create a 7940_7960_OTHER SIP dial rule.
2. Create a PLAR pattern called First PLAR.
3. Enter a pattern description called PLAR1.
4. Click the Add PLAR button, and the Button parameter displays.

Figure 19-3 7940_7960_OTHER Dial Rule Pattern for PLAR



SIP Dial Rule Configuration

Status
Update successful

SIP Dial Rule Information
Name* First PLAR
Description
Dial Pattern 7940_7960_OTHER

Pattern Information

Description	Delete Pattern	Dial Parameter	Value	Delete Parameter
PLAR1	□	Button		

Pattern Addition
Pattern Description

*- indicates required item.

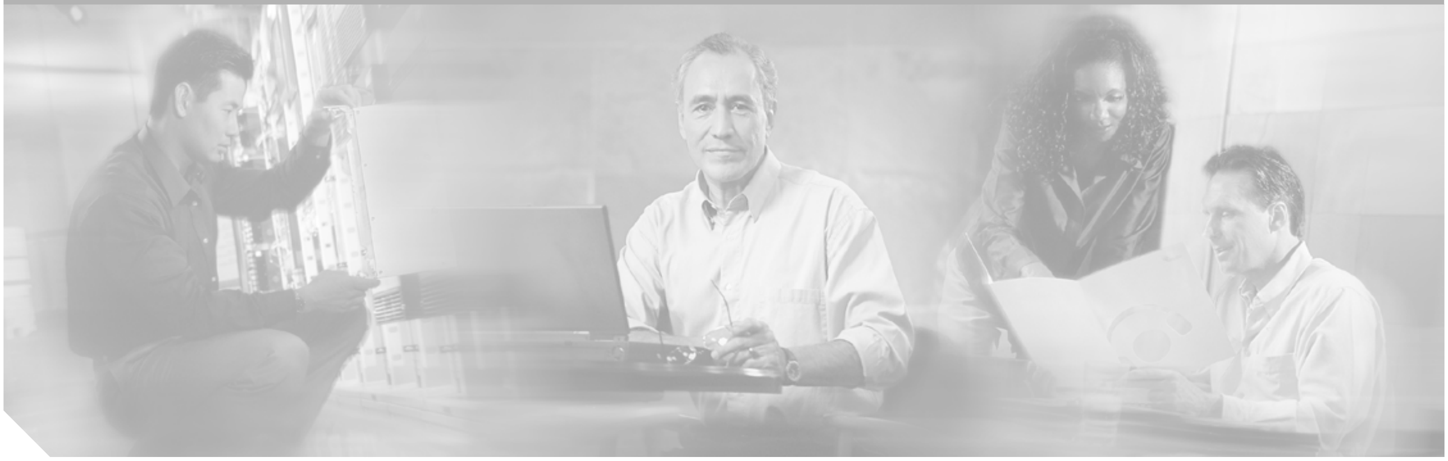
Where to Find More Information

Related Topic

- TFTP Process Overview for Cisco SIP IP Phones, page 10-3
- "Understanding Session Initiation Protocol (SIP)" section on page 41-1
- Directory Lookup Dial Rules Configuration, *Cisco Unified CallManager Administration Guide*
- Configuring Dial Rules, *Cisco Unified CallManager Administration Guide*
- Application Dial Rule Configuration Settings, *Cisco Unified CallManager Administration Guide*
- Configuring SIP Dial Rules, *Cisco Unified CallManager Administration Guide*
- SIP Dial Rule Configuration Settings, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco Unified CallManager Features and Services Guide*



PART 4

LDAP Directory and User Configuration

CHAPTER 20

Understanding the Directory

Directories comprise specialized databases that are optimized for a high number of reads and searches and occasional writes and updates. Directories typically store data that does not change often, such as employee information, user privileges on the corporate network, and so on.

Because directories are extensible, you can modify and extend the type of information that is stored in them. The term directory schema refers to the type of stored information and the rules that it obeys. Many directories provide methods for extending the directory schema to accommodate information types that different applications define. This capability enables enterprises to use the directory as a central repository for user information.

The Lightweight Directory Access Protocol (LDAP) provides applications with a standard method for accessing and potentially modifying the information that is stored in the directory. This capability enables companies to centralize all user information in a single repository, available to several applications, with a reduction in maintenance costs through the ease of adds, moves, and changes.

This chapter covers the main principles for synchronizing Cisco Unified CallManager with a corporate LDAP directory. The chapter also discusses the administrator’s choice not to synchronize with a corporate LDAP directory and the consequences of that choice of configuration. The chapter also summarizes considerations for providing Cisco Unified Communications endpoints, such as Cisco Unified IP Phones and Cisco IP SoftPhone, with access to a corporate LDAP directory.

The following list summarizes the changes in directory functionality from previous releases of Cisco Unified CallManager:

- The directory component has been decoupled from Cisco Unified CallManager to ensure high Cisco Unified CallManager availability independent of the corporate directory.
- Cisco Unified CallManager and related applications store all application data in the local database instead of in an embedded directory. The embedded directory gets removed and Cisco Unified CallManager supports synchronization with the customer directory.

This chapter includes the following topics:

- Cisco Unified CallManager and the Corporate LDAP Directory, page 20-2
- Directory Access, page 20-3
- DirSync Service, page 20-3
- Data Migration Assistant, page 20-4
- Authentication, page 20-4
- Using the Cisco Unified CallManager Database Versus the Corporate LDAP Directory, page 20-5
- Directory Access for Cisco Unified Communications Endpoints, page 20-5

- LDAP Directory Configuration Checklist, page 20-6
- Where to Find More Information, page 20-7

The considerations that this chapter presents apply to Cisco Unified CallManager as well as the following applications that are bundled with it: Cisco Extension Mobility, Cisco WebDialer, Bulk Administration Tool, and Real-Time Monitoring Tool.

For all other Cisco voice applications, refer to the respective product documentation that is available at

http://www.cisco.com

In particular, for Cisco Unity, refer to the *Cisco Unity Design Guide* and to the following white papers: *Cisco Unity Data and the Directory*, *Active Directory Capacity Planning*, and *Cisco Unity Data Architecture and How Cisco Unity Works*.

Cisco Unified CallManager and the Corporate LDAP Directory

Administrators access directory information about end users from the Cisco Unified CallManager Administration End User Configuration window (**User Management > End User**). Administrators use this window to add, update, and delete user information such as user ID, password, and device association, but only if synchronization from the LDAP Server is not enabled (that is, if the Enable Synchronizing from LDAP Server check box is not checked in the Cisco Unified CallManager Administration LDAP System window).

Applications and Services That Use the Database

The following Cisco Unified CallManager applications and services use the database for user and other types of information:

- Bulk Administration Tool (BAT)
- Tool for Auto-Registered Phone Support (TAPS)
- AXL
- Cisco Extension Mobility
- Cisco Unified CallManager User Options
- Cisco Conference Connection
- CTIManager
- CDR Analysis and Reporting (CAR)
- Cisco Unified CallManager Assistant
- Cisco Customer Response Solutions (CRS)
- Cisco Emergency Responder (CER)
- Cisco Unified IP Phone Services
- Personal Address Book (PAB)
- FastDials
- Cisco WebDialer
- Cisco IP Communicator
- Cisco Unified CallManager Attendant Console

Directory Access

The following definition applies throughout this chapter:

- Directory access refers to the ability of Cisco IP Telephony endpoints, such as Cisco IP Phones and Cisco IP SoftPhone, to access a corporate LDAP directory.

Figure 20-1 Directory Access for Cisco Unified Communications Endpoints

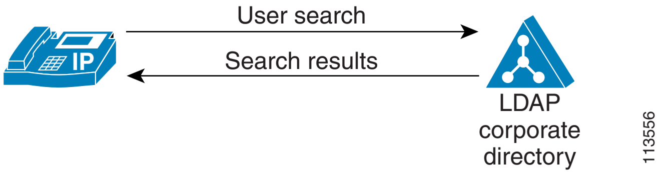


Figure 20-1 illustrates directory access as it is defined in this chapter. In this example, a Cisco Unified IP Phone gets access. The client application performs a user search against an LDAP directory, such as the corporate directory of an enterprise, and receives several matching entries. The Cisco IP Phone user can then select one entry and use it to dial the corresponding person from the Cisco IP Phone.

Note Directory access, as defined here, involves only read operations on the directory and does not require that the administrator make any directory schema extensions or other configuration changes.

DirSync Service

The DirSync application performs the synchronization of data in the Cisco Unified CallManager database with the customer LDAP directory information. Cisco Unified CallManager administrators set up the DirSync service by first configuring the LDAP-directory-related Cisco Unified CallManager windows. The following windows apply:

- LDAP System (**System > LDAP System**)
- LDAP Directory (**System > LDAP Directory**)

DirSync allows Cisco Unified CallManager to synchronize the data from corporate directories to Cisco Unified CallManager. DirSync allows synchronization from Microsoft Active Directory (AD) or Netscape/iPlanet Directory to the Cisco Unified CallManager database.

Note A DirSync that is invoked for Microsoft Active Directory performs a complete (total) synchronization of data. A DirSync that is invoked for Netscape Directory performs an incremental synchronization.

DirSync allows the following options:

- Automatic synchronization, which synchronizes the data at regular intervals
- Manual Synchronization, which allows forcing the synchronization
- Stop Synchronization, which stops the current synchronization. If synchronization is in progress, check for agreement.

Note When directory synchronization is enabled, Cisco Unified CallManager Administration cannot update any user information that is synchronized from the customer's Corporate Directory.

DirSync Service Parameters

You can configure service parameters for the DirSync service. Use the **System > Service Parameters** menu option in Cisco Unified CallManager Administration. On the window that displays, choose a server in the Server drop-down list box. Choose the Cisco DirSync service in the Service drop-down list box. The Service Parameter Configuration window allows configuration of the DirSync service parameters.

For more information about the DirSync service, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide.*

Data Migration Assistant

The Cisco Unified CallManager Data Migration Assistant (DMA) provides conversion of Cisco Unified CallManager 4.x data to a format that is compatible with Cisco Unified CallManager 5.0.

For details on obtaining, installing, and using DMA, refer to the *Cisco Unified CallManager Data Migration Assistant 1.0 User Guide*.

Authentication

The authentication process verifies the identity of the user by validating the user ID and password before granting access to the system. Verification takes place against the existing database or the LDAP corporate directory.

The system makes authentication, which the Cisco Unified CallManager administrator makes available in the LDAP Authentication window, available only if LDAP synchronization is enabled in the LDAP System window. If synchronization and authentication are both enabled, the following actions take place:

- The system always authenticates application users against the Cisco Unified CallManager database. When both synchronization and authentication are enabled, the user gets authenticated against the corporate directory. Thus, users need to use their corporate directory password.
- If only synchronization is enabled (and authentication is not enabled), users get authenticated against the Cisco Unified CallManager database. In this case, the administrator can configure a password by using the Cisco Unified CallManager Administration End User Configuration window. The default password specifies *ciscocisco*.

Using the Cisco Unified CallManager Database Versus the Corporate LDAP Directory

Two options exist for using directory information:

- To use only the Cisco Unified CallManager database for users, which is the default functionality when you install Cisco Unified CallManager, Release 5.0, create users with End User Configuration to add to the database (password, names, device association, and so forth). Authentication takes place against the information that is configured in Cisco Unified CallManager Administration. End users and administrators can make password changes if this method is used. This method does not entail LDAP synchronization.
- To use the Corporate LDAP directory (either Microsoft Active Directory or Netscape Directory) with Cisco Unified CallManager, the following steps must take place:
  - For users to use their LDAP corporate directory passwords, the Cisco Unified CallManager administrator must configure LDAP authentication (System > LDAP > LDAP Authentication).
  - Administrators cannot configure LDAP authentication unless they first configure LDAP synchronization. Doing so blocks further End User configuration.

    Note Keep in mind that configuring authentication is optional. If authentication is not enabled, administrators and end users have two passwords, an Active Directory or Netscape Directory password and a Cisco Unified CallManager password, which is *ciscocisco* by default.

Directory Access for Cisco Unified Communications Endpoints

The guidelines in this section apply regardless of whether Cisco Unified CallManager or other Cisco Unified Communications applications have been synchronized with a corporate directory. The end-user perception in both cases remains the same because the differences affect only how applications store their user information and how such information is kept consistent across the network.

The following sections summarize how to configure corporate directory access to any LDAPv3-compliant directory server for XML-capable phones such Cisco IP Phone models 7940, 7960, and so on.

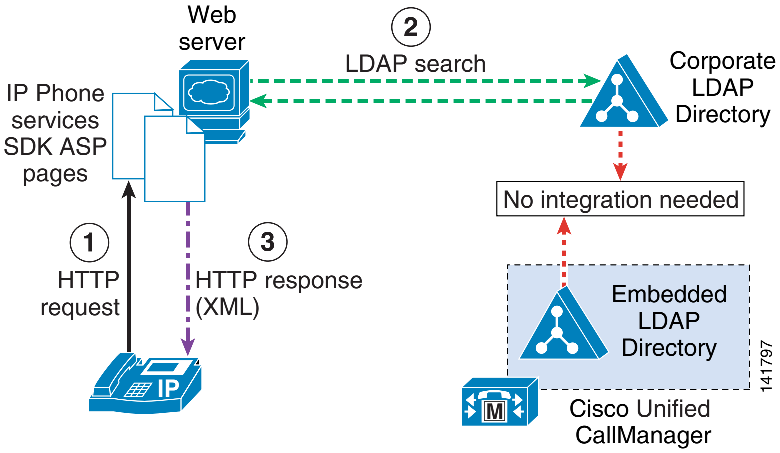
Note Cisco IP SoftPhone, Release 1.2 and later, includes a built-in mechanism to access and search LDAP directories, as does the Cisco IP Communicator. Refer to the product documentation for details on how to configure this feature.

Directory Access for Cisco IP Phones

XML-capable Cisco Unified IP Phones (such as models 7940, 7960, and so on) can search a corporate LDAP directory when a user presses the Directories button on the phone. The IP phones use HyperText Transfer Protocol (HTTP) to send requests to a web server. The responses from the web server must contain some specific Extensible Markup Language (XML) objects that the phone can interpret and display. In the case of a corporate directory search, the web server operates as a proxy by receiving the request from the phone and translating it into an LDAP request, which is in turn sent to the corporate directory server. After being encapsulated in the appropriate XML objects, the response gets interpreted and sent back to the phone.

Figure 20-2 illustrates this mechanism in a deployment where Cisco Unified CallManager has not been synchronized with the corporate directory. In this scenario, the message exchange does not involve Cisco Unified CallManager.

Figure 20-2 Message Exchange for Cisco Unified IP Phone Corporate Directory Access Without Directory Synchronization



You can configure the proxy function that the web server provided by using the Cisco Unified IP Phone Services Software Development Kit (SDK) version 2.0 or later, which includes the Cisco LDAP Search Component Object Model (COM) server.

In addition, directory access for Cisco Unified IP Phones includes the following characteristics:

- The system supports all LDAPv3-compliant directories.
- Cisco Unified CallManager user preferences (speed dials, call forward all, personal address book) do not get synchronized with the corporate LDAP directory. Therefore, users have a separate login and password to access the Cisco Unified CallManager User Options window.

LDAP Directory Configuration Checklist

Table 20-1 lists the general steps and guidelines for configuring LDAP directory information.

Table 20-1 User Directory Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Use the LDAP System windows to configure LDAP system settings.	LDAP System Configuration, *Cisco Unified CallManager Administration Guide*
Step 2	Use the LDAP Directory windows to configure LDAP directory settings.	LDAP Directory Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Use the LDAP Authentication windows to configure LDAP authentication settings.	LDAP Authentication Configuration, *Cisco Unified CallManager Administration Guide*

Table 20-1 User Directory Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 4	If directory synchronization is enabled, use the DirSync service to synchronize with the customer's corporate LDAP directory.	*Cisco Unified CallManager Serviceability System Guide* *Cisco Unified CallManager Serviceability Administration Guide*
Step 5	To convert Cisco Unified CallManager 4.x data to a format that is compatible with Cisco Unified CallManager 5.0, use the Cisco Unified CallManager Data Migration Assistant (DMA).	*Cisco Unified CallManager Data Migration Assistant 1.0 User Guide*

Where to Find More Information

Related Topics

- LDAP System Configuration, *Cisco Unified CallManager Administration Guide*
- LDAP Directory Configuration, *Cisco Unified CallManager Administration Guide*
- LDAP Authentication Configuration, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Data Migration Assistant 1.0 User Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- Cisco Unified CallManager Groups, page 5-3
- System Configuration Checklist, page 5-17
- Application Users and End Users, page 21-1
- Application User Configuration, *Cisco Unified CallManager Administration Guide*
- End User Configuration, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- *Installing Cisco Unified CallManager Release 5.0(4)*
- *Cisco Unified Communications Solution Reference Network Design for Cisco Unified CallManager*

CHAPTER 21

Application Users and End Users

The Application User Configuration window and the End User Configuration window in Cisco Unified CallManager Administration allow the administrator to add, search, display, and maintain information about Cisco Unified CallManager application users and end users. This chapter describes the options for managing user directory information.

Refer to the "Application User Configuration" section of the *Cisco Unified CallManager Administration Guide* for more procedures on adding application users and configuring their application profiles.

Refer to the "End User Configuration" section of the *Cisco Unified CallManager Administration Guide* for procedures on managing and updating end user information.

This chapter includes the following topics:

- How Cisco Unified CallManager JTAPI Uses the Directory, page 21-1
- Application Users, page 21-2
- End Users, page 21-2
- Application Profiles, page 21-3
- Device Association, page 21-3
- Cisco Extension Mobility Profiles, page 21-4
- Cisco IP SoftPhone Profiles, page 21-5
- Managing Application User and End User Configuration Checklist, page 21-5
- Where to Find More Information, page 21-6

How Cisco Unified CallManager JTAPI Uses the Directory

Cisco Unified CallManager Java Telephony Applications Programming Interface (JTAPI) uses the directory to determine which devices it can control and provides an interface method for getting the Media Access Control (MAC) address of the calling party, such as a user who is initiating the Cisco Extension Mobility Login.

After you install Cisco JTAPI, you have access to the Cisco Unified CallManager directory. The directory stores parameters that initialize JTAPI, user profiles, application logic, and network-specific configuration information, such as the location of network resources and system administrator authentication.

Application Users

Application user configuration allows updates to the application users that are associated with Cisco Unified CallManager. By default, Cisco Unified CallManager Administration includes these application users:

- CCMAdministrator
- CCMSysUser

You cannot delete these default application users, but you can change their passwords and modify the lists of devices that they control.

Note By default, the CCMAdministrator password specifies *ciscocisco*. The person that uses this application user ID should change the default password for this application user as soon as possible after logging on.

To configure application user information, use the **User Management > Application User** menu option in Cisco Unified CallManager Administration. Refer to the "Application User Configuration" section in the *Cisco Unified CallManager Administration Guide* for details.

End Users

You can add new end users through Cisco Unified CallManager Administration only when synchronization with the corporate LDAP server is disabled. When synchronization is disabled, you can add new users and you can change the settings of existing users including the user ID. If synchronization is enabled, you cannot add new users and you cannot change existing user IDs. You can, however, change all other settings for existing end users.

To check whether configuration is enabled, use the **System > LDAP > LDAP System** menu option in Cisco Unified CallManager Administration. If the Enable Synchronizing from LDAP Server check box is not checked, synchronization is not in effect. Refer to the "LDAP System Configuration" in the *Cisco Unified CallManager Administration Guide* for details.

To configure end user information, use the **User Management > End User** menu option in Cisco Unified CallManager Administration. Refer to the "End User Configuration" section in the *Cisco Unified CallManager Administration Guide* for details.

You can use the End User, Phone, DN, and LA Configuration window to add a new user and a new phone at the same time. You can associate a directory number and line appearance for the new end user by using the same window. To access the End User, Phone, DN, and LA Configuration window, choose the **User Management > User/Phone Add** menu option. Refer to "User/Phone Add Configuration" in the *Cisco Unified CallManager Administration Guide* for configuration details.

Note The End User, Phone, DN, and LA Configuration window only allows addition of a new end user and a new phone. The window does not allow entry of existing end users or existing phones.

Application Profiles

After you add a new application user, the CAPF Information pane on the Application User Configuration window allows you to configure the CAPF profile that is associated with the application user. For more information about the application user CAPF profile, see the "Application User CAPF Profile Configuration" chapter of the *Cisco Unified CallManager Administration Guide*.

After you add a new end user, options in the Extension Mobility pane and the CAPF Information pane on the End User Configuration window allow you to configure the end user application profiles. These profiles allow each end user to personalize Cisco Extension Mobility and to update the end user CAPF profile. For more information about the end user CAPF profile, see the "End User CAPF Profile Configuration" chapter of the *Cisco Unified CallManager Administration Guide*.

For information on configuring application profiles for application users, refer to the "Configuring Application Profiles for Application Users" section of the *Cisco Unified CallManager Administration Guide*. For information on configuring application profiles for end users, refer to the "Configuring User-Related Information for End Users" section of the *Cisco Unified CallManager Administration Guide*.

Device Association

Associating devices to an application user or to an end user gives the user control over specified devices. Application users and end users control some devices, such as phones. Applications that are identified as end users control other devices, such as CTI ports. When application users or end users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding. See the following topics for additional information about associating devices with users:

- Device Association for Application Users, page 21-3
- Device Association for End Users, page 21-4

Device Association for Application Users

Use the Device Information portion of the Application User Configuration window to associate devices with an existing application user. The Available Devices pane lists the devices that are available for association with an application user. The Available Devices pane lists devices by device name. To search for additional devices to associate with an application user, use the **Find more Phones**, **Find more Route Points**, and **Find more Pilot Points** buttons. Each button opens a popup window where you can limit the list of devices by entering search criteria based on all or part of the device name, description, or other parameter. To limit the list of available devices to a specific selection, enter the criteria by which you want to search by using the following methods:

- Choose a search parameter, such as device name, description, or directory number.
- Choose the comparison operator, such as begins with.
- Enter search text.

For example, to list all extensions that begin with '5,' you would choose Directory Number begins with and then enter **5** in the text box.

After you have specified the search criteria to display devices, all matching, available devices display in the Search Results. You can navigate the list by using the buttons at the bottom of the window.

You can associate one or more devices to the application user by checking that check box next to that device. If a device has multiple extensions that are associated with it, each line extension displays in the list. You need to choose only one line extension to choose all the lines that are associated with that device.

For more information on assigning devices to an application user, refer to "Associating Devices to an Application User" in the *Cisco Unified CallManager Administration Guide*.

Device Association for End Users

Use the Device Associations portion of the End User Configuration window to associate devices with an existing end user. The Controlled Devices pane lists the devices that are already associated with an end user. The Controlled Devices pane lists devices by device name. To search for additional devices to associate with an end user, use the **Device Association** button. This button opens the User Device Association window where you can limit the list of devices by entering search criteria based on all or part of the device name or description. To limit the list of available devices to a specific selection, enter the criteria by which you want to search by using the following methods:

- Choose a search parameter, such as device name or description.
- Choose the comparison operator, such as begins with.
- Enter search text.

After you have specified the search criteria to display devices, all matching, available devices display in the Device association for (this end user) portion of the User Device Association window. You can navigate the list by using the buttons at the bottom of the window.

You can associate one or more devices to the end user by checking that check box next to that device. If a device has multiple extensions that are associated with it, each line extension displays in the list. You need to choose only one line extension to choose all the lines that are associated with that device.

For a detailed procedure for assigning devices to an end user, refer to "Associating Devices to an End User" in the *Cisco Unified CallManager Administration Guide*.

Cisco Extension Mobility Profiles

Use Cisco Extension Mobility to configure a Cisco Unified IP Phone to appear temporarily as a user phone. The user can log in to a phone, and the user extension mobility profile (including line and speed-dial numbers) resides on the phone. This feature applies primarily in environments where users are not permanently assigned to physical phones.

User device profiles and device profile defaults support the Cisco Extension Mobility feature. The user device profile includes the following information:

- Device Profile Information—Includes Device Type, User Device Profile Name, Description, User Hold Audio Source, and User Locale.
- Phone Button Information—Includes Phone Button Template for the device type.
- Softkey Template Information—Includes list of available softkey templates.
- Expansion Module Information—Includes Cisco IP Phone add-on modules such as the Cisco Model 7914 Expansion Module.

- Multilevel Precedence and Preemption Information—Includes MLPP domain, indication, and preemption settings.
- Logged-Out Default Profile Information—Includes Log In User ID

An authentication scheme authenticates the user. The workflow engine sends an XML string through an HTTP post request to the Login Service. The string contains the following items:

- User name and password of the login application
- Device name that is based on the MAC address of the device on which the user wants their profile to reside

A dialog prompt displays on the device of the user.

For more information on Cisco Extension Mobility, refer to Cisco Extension Mobility in the *Cisco Unified CallManager Features and Services Guide*.

Cisco IP SoftPhone Profiles

You can associate a device (line) to a user as a Cisco IP SoftPhone. This enables users to use their desktop PC to place and receive telephone calls and to control an IP telephone.

For more information on Cisco IP SoftPhone, refer to the *Cisco IP SoftPhone Administrator Guide.*

Managing Application User and End User Configuration Checklist

Table 21-1 lists the general steps and guidelines for managing application user and end user information.

Table 21-1 Application User and End User Configuration Checklist

Configuration Steps		**Related procedures and topics**
Step 1	Search for an application user.	Finding an Application User, *Cisco Unified CallManager Administration Guide*
Step 2	Add an application user as needed.	Adding an Application User, *Cisco Unified CallManager Administration Guide*
Step 3	Configure the application profiles for application users.	Application Profiles, *Cisco Unified CallManager Administration Guide*
Step 4	Search for an end user.	Finding an End User, *Cisco Unified CallManager Administration Guide*

Table 21-1 Application User and End User Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 5	Add an end user as needed.	Adding an End User, *Cisco Unified CallManager Administration Guide*
Step 6	Configure the application profiles for end users.	Configuring User-Related Information for End Users, *Cisco Unified CallManager Administration Guide*

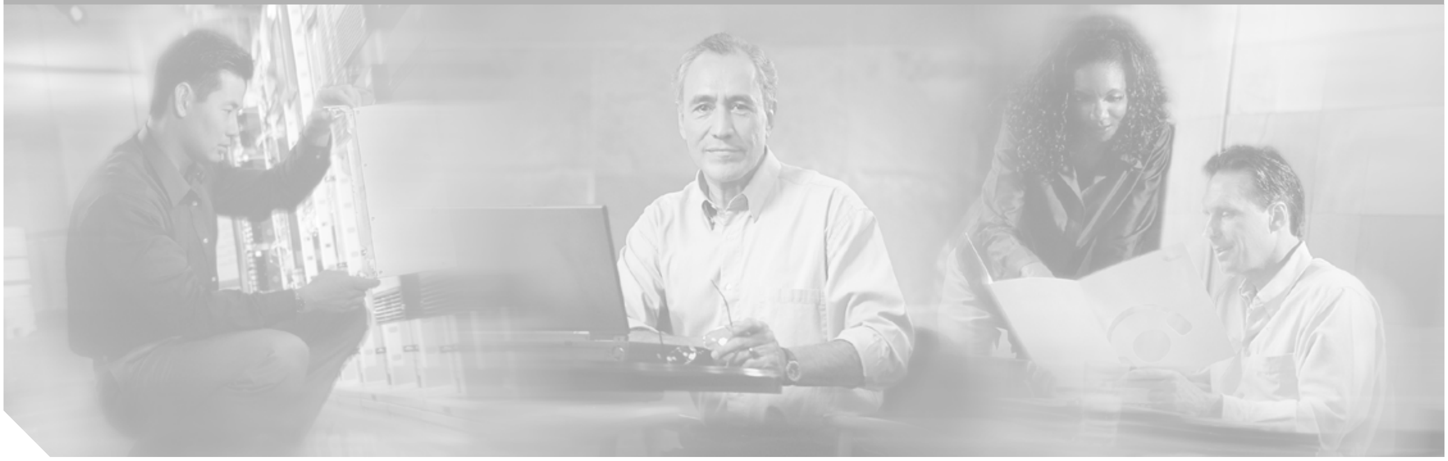
Where to Find More Information

Related Topics

- Application User Configuration, *Cisco Unified CallManager Administration Guide*
- End User Configuration, *Cisco Unified CallManager Administration Guide*
- User/Phone Add Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*
- LDAP System Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Extension Mobility, *Cisco Unified CallManager Features and Services Guide*

Additional Cisco Documentation

- *Cisco IP SoftPhone Administrator Guide*
- *Cisco IP SoftPhone User Guide*
- *Cisco Unified CallManager Features and Services Guide*
- Cisco IP Phone user documentation and release notes (all models)



PART 5

Media Resources

Media Resource Management

Cisco Unified Communications functionality requires the use of media resources. Media resources provide services such as annunciator, transcoding, conferencing, music on hold, and media termination. In previous releases, only the local Cisco Unified CallManager with which the media resources registered could access these resources that are but not available to all Cisco Unified CallManagers within the cluster. The media resource manager allows all Cisco Unified CallManagers within the cluster to share these media resources.

The media resource manager enhances Cisco Unified CallManager features by making Cisco Unified CallManager more readily able to deploy annunciator, media termination point, transcoding, conferencing, and music on hold services. Distribution throughout the cluster uses resources to their full potential, which makes them more efficient and more economical.

This chapter covers the following topics:

- Understanding Media Resources, page 22-1
- Media Resource Groups, page 22-3
- Media Resource Group Lists, page 22-4
- Dependency Records, page 22-6
- Media Resource Group and Media Resource Group List Configuration Checklist, page 22-6
- Where to Find More Information, page 22-7

Understanding Media Resources

Media resource management provides access to media resources for all Cisco Unified CallManagers in a cluster. Every Cisco Unified CallManager contains a software component called a media resource manager. The media resource manager locates the media resource that is necessary to connect media streams to complete a feature.

The media resource manager manages the following media resource types:

- Music On Hold (MOH) server
- Unicast conference bridge (CFB)
- Media termination point (MTP)
- Transcoder (XCODE)
- Annunciator (ANN)

The following reasons explain why resources are shared:

- To allow both hardware and software devices to coexist within a Cisco Unified CallManager
- To enable Cisco Unified CallManager to share and access resources that are available in the cluster
- To enable Cisco Unified CallManager to do load distribution within a group of similar resources
- To enable Cisco Unified CallManager to allocate resources on the basis of user preferences

Initialization of the Cisco Unified CallManager creates a media resource manager. Each media termination point, music on hold, transcoder, conference bridge, and annunciator device that is defined in the database registers with the media resource manager. The media resource manager obtains a list of provisioned devices from the database and constructs and maintains a table to track these resources. The media resource manager uses this table to validate registered devices. The media resource manager keeps track of the total devices that are available in the system, while also tracking the devices that have available resources.

When a media device registers, Cisco Unified CallManager creates a controller to control this device. After the device is validated, the system advertises its resources throughout the cluster. This mechanism allows the resource to be shared throughout the cluster.

Resource reservation takes place based on search criteria. The given criteria provide the resource type and the media resource group list. When the Cisco Unified CallManager no longer needs the resource, resource deallocation occurs. Cisco Unified CallManager updates and synchronizes the resource table after each allocation and deallocation.

The media resource manager interfaces with the following major components:

- Call control
- Media control
- Media termination point control
- Unicast bridge control
- Music on hold control
- Annunciator control

Call Control

Call control software component performs call processing, including setup and tear down of connections. Call control interacts with the feature layer to provide services like transfer, hold, conference, and so forth. Call control interfaces with the media resource manager when it needs to locate a resource to set up conference call and music on hold features.

Media Control

Media control software component manages the creation and teardown of media streams for the endpoint. Whenever a request for media to be connected between devices is received, depending on the type of endpoint, media control sets up the proper interface to establish a stream.

The media layer interfaces with the media resource manager when it needs to locate a resource to set up a media termination point or transcoding.

Media Termination Point Control

Media termination point (MTP) provides the capability to bridge an incoming H.245 stream to an outgoing H.245 stream. Media termination point maintains an H.245 session with an H.323 endpoint when the streaming from its connected endpoint stops. Media termination point currently supports only codec G.711. Media termination point can also transcode G.711 a-law to mu-law.

The Media Resource Manager (MRM) provides resource reservation of transcoders within a Cisco Unified CallManager cluster. Cisco Unified CallManager supports simultaneous registration of both the MTP and transcoder and concurrent MTP and transcoder functionality within a single call. A transcoder takes the stream of one codec and transcodes (converts) it from one compression type to another compression type. For example, it could take a stream from a G.711 codec and transcode (convert) it in real time to a G.729 stream. In addition, a transcoder provides MTP capabilities and may be used to enable supplementary services for H.323 endpoints when required.

For each media termination point device and each transcoder that is registered with Cisco Unified CallManager, Cisco Unified CallManager creates a media termination point control process. This media termination point control process registers with the device manager when it initializes. The device manager advertises the availability of the media termination point control processes throughout the cluster.

Annunciator Control

An annunciator enables Cisco Unified CallManager to play pre-recorded announcements (.wav files) and tones to Cisco Unified IP Phones, gateways, and other configurable devices. The annunciator, which works with Cisco Unified CallManager Multilevel Precedence and Preemption, enables Cisco Unified CallManager to alert callers as to why the call fails. Annunciator can also play tones for some transferred calls and some conferences.

For each annunciator device that is registered with Cisco Unified CallManager, Cisco Unified CallManager creates an annunciator control process. This annunciator control process registers with the device manager when it initializes. The device manager advertises the availability of the annunciator control process throughout the cluster.

Unicast Bridge Control

A unicast bridge (CFB) provides the capability to mix a set of incoming unicast streams into a set of composite output streams. Unicast bridge provides resources to implement ad hoc and meet-me conferencing in the Cisco Unified CallManager.

For each unicast bridge device that is registered with Cisco Unified CallManager, Cisco Unified CallManager creates a unicast control process. This unicast control process registers with the device manager when it initializes. The device manager advertises the availability of unicast stream resources throughout the cluster.

Music On Hold Control

Music on hold (MOH) provides the capability to redirect a party on hold to an audio server. For each music on hold server device that is registered with Cisco Unified CallManager, Cisco Unified CallManager creates a music on hold control process. This music on hold control process registers with the device manager when it initializes. The device manager advertises the availability of music on hold resources throughout the cluster. Music on hold supports both unicast and multicast audio sources.

Media Resource Groups

Cisco Unified CallManager media resource groups and media resource group lists provide a way to manage resources within a cluster. Use these resources for conferencing, transcoding, media termination, and music on hold (MOH).

Media resource groups define logical groupings of media servers. You can associate a media resource group with a geographical location or a site as desired. You can also form media resource groups to control the usage of servers or the type of service (unicast or multicast) that is desired.

After media resources are configured, if no media resource groups are defined, all media resources belong to the default group, and, as such, all media resources are available to all Cisco Unified CallManagers within a given cluster.

Tip Deactivating the Cisco IP Voice Media Streaming Application deletes associated devices (Annunciator, Conference Bridge, Music-on-Hold, and Media Termination Point) from media resource groups. If the deletion results in an empty media resource group, you cannot deactivate the service; in this case, you must delete the media resource group before deactivating the service.

The following rules govern selection of a resource from a media resource group in a media resource group list:

- Search the first media resource group in a media resource group list to find the requested resource. If located, return the resource ID.
- If the requested resource is not found, search the next media resource group in the media resource group list. Return the resource ID if a match is found.
- If no resource of the requested type is available in any media resource group in a media resource group list, the resource manager attempts to use the resource in the default group.

Example

The default media resource group for a Cisco Unified CallManager comprises the following media resources: MOH1, MTP1, XCODE1, XCODE2, XCODE3. For calls that require a transcoder, this Cisco Unified CallManager distributes the load evenly among the transcoders in its default media resource group. The following allocation order occurs for incoming calls that require transcoders:

```
Call 1 - XCODE1
Call 2 - XCODE2
Call 3 - XCODE3
Call 4 - XCODE1
Call 5 - XCODE2
Call 6 - XCODE3
Call 7 - XCODE1
```

Media Resource Group Lists

Media resource group lists specify a list of prioritized media resource groups. An application can select required media resources from among the available resources according to the priority order that is defined in the media resource group list. Media resource group lists, which are associated with devices, provide media resource group redundancy.

The following rules govern selection of media resource group lists:

- A media resource group list, which is configured in the Media Resource Group List Configuration window, gets assigned to either a device or to a device pool.
- Call processing uses a media resource group list in the device level if the media resource group list is selected. If a resource is not found, call processing may retrieve it from the default allocation.
- Call processing uses media resource group list in the device pool only if no media resource group list is selected in the device level. If a resource is not found, call processing may retrieve it from the default allocation.

Example of Using Media Resource Group List to Group Resources by Type

Assign all resources to three media resource groups as listed:

- SoftwareGroup media resource group: MTP1, MTP2, SW-CONF1, SWCONF2
- HardwareGroup media resource group: XCODE1, XCODE2, HW-CONF1, HW-CONF2
- MusicGroup media resource group: MOH1, MOH2

Create a media resource group list called RESOURCE_LIST and assign the media resource groups in this order: SoftwareGroup, HardwareGroup, MusicGroup.

Result: With this arrangement, when a conference is needed, Cisco Unified CallManager allocates the software conference resource first; the hardware conference does not get used until all software conference resources are exhausted.

Example of Using Media Resource Group List to Group Resources by Location

Assign resources to four media resource groups as listed:

- DallasSoftware: MTP1, MOH1, SW-CONF1
- SanJoseSoftware: MTP2, MOH2, SW-CONF2
- DallasHardware: XCODE1, HW-CONF1
- SanJoseHardware: XCODE2, HW-CONF2

CM1 and CM2 designate Cisco Unified CallManagers.

Create a DALLAS_LIST media resource group list and assign media resource groups in this order: DallasSoftware, DallasHardware, SanJoseSoftware, SanJoseHardware

Create a SANJOSE_LIST media resource group list and assign media resource groups in this order: SanJoseSoftware, SanJoseHardware, DallasSoftware, DallasHardware.

Assign a phone in Dallas CM1 to use DALLAS_LIST and a phone in San Jose CM2 to use SANJOSE_LIST.

Result: With this arrangement, phones in CM1 use the DALLAS_LIST resources before using the SANJOSE_LIST resources.

Example of Using Media Resource Group List to Restrict Access to Conference Resources

Assign all resources to four groups as listed, leaving no resources in the default group:

- MtpGroup: MTP1, MTP2
- ConfGroup: SW-CONF1, SW-CONF2, HW-CONF1, HW-CONF2
- MusicGroup: MOH1, MOH2
- XcodeGroup: XCODE1, XCODE2

Create a media resource group list that is called NO_CONF_LIST and assign media resource groups in this order: MtpGroup, XcodeGroup, MusicGroup.

In the device configuration, assign the NO_CONF_LIST as the device media resource group list.

Result: The device cannot use conference resources. This means that only media termination point, transcoder, annunciator, and music resources are available to the device.

Dependency Records

To find out which media resource group lists are associated the media resource groups, click the Dependency Records link that displays in the Cisco Unified CallManager Administration Media Resource Group Configuration window. To find out more information about the media resource group list, click the record type, and the Dependency Records Details window displays.

To find out which phones or trunks are associated with media resource group lists, click the Dependency Records link that displays in the Cisco Unified CallManager Administration Media Resource Group List 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 Dependency Records in the *Cisco Unified CallManager Administration Guide*.

Media Resource Group and Media Resource Group List Configuration Checklist

Table 22-1 provides a checklist to configure media resource groups and media resource group lists.

Table 22-1 Media Resource Group/Media Resource Group List Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Create a media resource group.	Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide*
Step 2	Assign device to the media resource group. (Order has no significance.)	Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Create a media resource group list. (Order has significance.)	Media Resource Group List Configuration, *Cisco Unified CallManager Administration Guide*
Step 4	Assign a media resource group to a media resource group list.	Media Resource Group List Configuration, *Cisco Unified CallManager Administration Guide*
Step 5	Assign a media resource group list to a device or device pool.	Device Defaults Configuration, *Cisco Unified CallManager Administration Guide* Device Pool Configuration, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Additional Cisco Documentation

- Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide*
- Media Resource Group List Configuration, *Cisco Unified CallManager Administration Guide*
- Music On Hold Audio Source Configuration, *Cisco Unified CallManager Features and Services Guide*
- Music On Hold Server Configuration, *Cisco Unified CallManager Features and Services Guide*
- Accessing Dependency Records, *Cisco Unified CallManager Administration Guide*
- Media Termination Points, page 27-1
- Annunciator, page 23-1
- Conference Bridges, page 24-1
- Transcoders, page 25-1

CHAPTER 23

Annunciator

An annunciator, an SCCP device that uses the Cisco IP Voice Media Streaming Application service, enables Cisco Unified CallManager to play pre-recorded announcements (.wav files) and tones to Cisco Unified IP Phones, gateways, and other configurable devices. The annunciator, which works with Cisco Unified CallManager Multilevel Precedence and Preemption, enables Cisco Unified CallManager to alert callers as to why the call fails. Annunciator can also play tones for some transferred calls and some conferences.

This section covers the following topics:

- Understanding Annunciators, page 23-1
- Planning Your Annunciator Configuration, page 23-2
- Annunciator System Requirements and Limitations, page 23-3
- Supported Tones and Announcements, page 23-4
- Dependency Records, page 23-5
- Annunciator Performance Monitoring and Troubleshooting, page 23-5
- Annunciator Configuration Checklist, page 23-5
- Where to Find More Information, page 23-6

Understanding Annunciators

In conjunction with Cisco Unified CallManager, the annunciator device provides multiple one-way, RTP stream connections to devices, such as Cisco Unified IP Phones and gateways.

To automatically add an annunciator to the Cisco Unified CallManager database, you must activate the Cisco IP Voice Media Streaming Application service on the server where you want the annunciator to exist in the cluster.

Note When you add a server, the annunciator device is automatically added for the new server. It will remain inactive until the Cisco IP Voice Media Streaming Application service is activated for the new server.

Cisco Unified CallManager uses SCCP messages to establish a RTP stream connection between the annunciator and the device. The annunciator plays the announcement or tone to support the following conditions:

- Announcement—Devices configured for Cisco Multilevel Precedence and Preemption
- Barge tone—Before a participant joins an ad hoc conference
- Ring back tone—When you transfer a call over the PSTN through an IOS gateway

  Annunciator plays the tone because the gateway cannot play the tone when the call is active.
- Ring back tone—When you transfer calls over an H.323 intercluster trunk
- Ring back tone—When you transfer calls to the SIP client from a SCCP phone

Tip For specific information about supported announcements and tones, see the "Supported Tones and Announcements" section on page 23-4.

Before the announcement/tone plays, the annunciator reads the following information from the annunciator.xml file in the Cisco Unified CallManager database:

- The TypeAnnouncements database table is read into memory cache to identify each announcement or tone supported by the annunciator.
- The user locale identifier for the phone, which is added to the database if you install the Cisco Unified CallManager Locale Installer on every server in the cluster
- The network locale identifier for the phone or gateway, which is added to the database if you install the Cisco Unified CallManager Locale Installer on every server in the cluster
- The device settings
- The user-configured service parameters

Planning Your Annunciator Configuration

Consider the following information before you plan your annunciator configuration. Use this information in conjunction with the "Annunciator System Requirements and Limitations" section on page 23-3.

- For a single annunciator, Cisco Unified CallManager sets the default to 48 simultaneous streams, as indicated in the annunciator service parameter for streaming values.

Caution Cisco recommends that you do not exceed 48 annunciator streams on a co-resident server where the Cisco Unified CallManager and Cisco IP Voice Media Streaming Application services run.

- You can change the default to best suit your network. For example, a 100-MB Network/NIC card can support 48 annunciator streams, while a 10-MB NIC card supports up to 24 annunciator streams. The exact number of annunciator streams that are available depends on the factors, such as the speed of the processor and network loading.
- If the annunciator runs on a standalone server where the Cisco CallManager service does not run, the annunciator can support up to 255 simultaneous announcement streams.
- If the standalone server has dual CPU and a high-performance disk system, the annunciator can support up to 400 simultaneous announcement streams.

Consider the following formula to determine the approximate number of annunciators that you need for your system. This formula assumes that the server can handle the default number of streams (48); you can substitute the default number for the number of streams that your server supports.

n/number of annunciator devices that you server supports

where:

n represents the number of devices that require annunciator support

Tip If a remainder exists in the quotient, consider adding another server to support an additional annunciator device. To perform this task, activate the Cisco IP Voice Media Streaming Application service on another server and update the configuration of the device, if you do not want to use the default settings.

Annunciator System Requirements and Limitations

The following system requirements and limitations apply to annunciator devices:

- For one annunciator device, activate only one Cisco IP Voice Media Streaming Application service in the cluster. To configure additional annunciators, you must activate the Cisco IP Voice Media Streaming Application service on additional Cisco Media Convergence Servers or Cisco-approved, third-party servers where Cisco Unified CallManager is installed in the cluster.

Caution Cisco strongly recommends that you do not activate the Cisco IP Voice Media Streaming Application service on a Cisco Unified CallManager with a high call-processing load.

- Each annunciator registers with only one Cisco Unified CallManager at a time. The system may have multiple annunciators depending on your configuration, each of which may register with different Cisco Unified CallManager servers.
- Each annunciator belongs to a device pool. The device pool associates the secondary (backup) Cisco Unified CallManager and the region settings.
- Each annunciator can support G.711 a-law, G.711 mu-law, wideband, and G.729 codec formats. A separate wav file exists for each codec that is supported.
- For information on the number of streams that are available for use, see the "Planning Your Annunciator Configuration" section on page 23-2.
- To manage the media resources in the cluster, you can add the annunciator to a Media Resource Group, and likewise, a Media Resource List.
- When you update the annunciator, the changes automatically occur when the annunciator becomes idle, when no active announcements are played.
- Cisco Unified CallManager provides annunciator resource support to a conference bridge under the following circumstances:
  - If the media resource group list that contains the annunciator is assigned to the device pool where the conference bridge exists.
  - If the annunciator is configured as the default media resource, which makes it available to all devices in the cluster.

  Cisco Unified CallManager does not provide annunciator resource support for a conference bridge if the media resource group list is assigned directly to the device that controls the conference.

Caution If you configured redundancy between Cisco Unified CallManager servers, all announcements that are playing during the failover drop. The annunciator does not preserve announcement streams during Cisco Unified CallManager failover.

Supported Tones and Announcements

Cisco Unified CallManager automatically provides a set of recorded annunciator announcements when you activate the Cisco IP Media Streaming Application service. No provision is provided to customize these announcements or to add new announcements.

Annunciator announcements, which consist of 1 or 2 wav files, support localization if you have installed the Cisco Unified CallManager Locale Installer and configured the locale settings for the Cisco Unified IP Phone or, if applicable, the device pool. Each announcement plays in its entirety.

Cisco Unified CallManager supports only one announcement per conference. During a conference if the system requests a new announcement while another announcement currently plays, the new announcement preempts the other announcement.

Annunciator supports the announcements in Table 23-1.

Table 23-1 Announcements

Condition	Announcement
An equal or higher precedence call is in progress.	Equal or higher precedence calls have prevented the completion of your call. Please hang up and try again. This is a recording.
A precedence access limitation exists.	Precedence access limitation has prevented the completion of your call. Please hang up and try again. This is a recording.
Someone attempted an unauthorized precedence level.	The precedence used is not authorized for your line. Please use an authorized precedence or ask your operator for assistance. This is a recording.
The call appears busy, or the administrator did not configure the directory number for call waiting or preemption.	The number you have dialed is busy and not equipped for call waiting or preemption. Please hang up and try again. This is a recording.
The system cannot complete the call.	Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording.
A service interruption occurred.	A service disruption has prevented the completion of your call. In case of emergency call your operator. This is a recording.

Annunciator supports the following tones:

- Busy tone
- Alerting/Ring back tone
- Conference barge-in tone

Dependency Records

To find which media resource groups include an annunciator device, choose Dependency Records from Related Links drop-down list box and click Go. The Dependency Records Summary window displays information about media resource groups that use the annunciator device. To find out more information about the media resource group, click the media resource group, 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" and "Deleting a Media Resource Group" in the *Cisco Unified CallManager Administration Guide*.

Annunciator Performance Monitoring and Troubleshooting

Performance Monitor counters for annunciator allow you to monitor the number of streams that are used, the streams that are currently active, the total number of streams that are available for use, the number of failed annunciator streams, the current connections to the Cisco Unified CallManager, and the total number of times a disconnection occurred from the Cisco Unified CallManager. When an annunciator stream is allocated or de-allocated, the performance monitor counter updates the statistic. For more information about performance monitor counters, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Cisco Unified CallManager writes all errors for the annunciator to the Event Viewer. In Cisco Unified CallManager Serviceability, you can set traces for the Cisco IP Voice Media Streaming Application service; to troubleshoot most issues, you must choose the Significant or Detail option for the service, not the Error option. Reset trace level to the Error option after you troubleshoot the issue.

Cisco Unified CallManager generates registration and connection alarms for annunciator in Cisco Unified CallManager Serviceability. For more information on alarms, refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System Guide*.

If you need technical assistance, use the Real-Time Monitoring Tool to retrieve the cms/sdi trace log files before you contact your Cisco Partner or the Cisco Technical Assistance Center (TAC).

Annunciator Configuration Checklist

Table 23-2 provides a checklist to configure an annunciator.

Table 23-2 Annunciator Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Determine the number of annunciator streams that are needed and the number of annunciators that are needed to provide these streams.	Planning Your Annunciator Configuration, page 23-2
Step 2	Verify that you have activated the Cisco IP Voice Media Streaming Application service on the server where you want the annunciator to exist.	*Cisco Unified CallManager Serviceability Administration Guide* *Cisco Unified CallManager Serviceability System Guide*

Table 23-2 Annunciator Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 3	Perform additional annunciator configuration tasks if you want to change the default settings.	Annunciator Configuration, *Cisco Unified CallManager Administration Guide*
Step 4	Add the new annunciators to the appropriate media resource groups and media resource lists.	Media Resource Management, page 22-1 Media Resource Group Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 5	Reset or restart the individual annunciator or all devices that belong to the media resource group/list.	Annunciator System Requirements and Limitations, page 23-3

Where to Find More Information

Related Topics

- Media Resource Management, page 22-1
- Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide*
- Multilevel Precedence and Preemption, *Cisco Unified CallManager Features and Services Guide*
- Annunciator Configuration, *Cisco Unified CallManager Administration Guide*

Conference Bridges

Conference Bridge for Cisco Unified CallManager designates a software or hardware application that is designed to allow both ad hoc and meet-me voice conferencing. Additional conference bridge types support other types of conferences, including video conferences. Each conference bridge can host several simultaneous, multiparty conferences.

Conference Bridge includes the following features:

- Creating a conference call
- Adding new participants to an existing conference call
- Ending a conference call
- Dropping conference participants
- Canceling a conference call
- Parking a conference call
- Transferring a conference call

This section covers the following topics:

- Understanding Conference Devices, page 24-1
- Conference Bridge Types in Cisco Unified CallManager Administration, page 24-4
- Using Different Conference Types: Meet Me and Ad Hoc, page 24-6
- Dependency Records, page 24-9
- Conference Bridge Performance Monitoring and Troubleshooting, page 24-10
- Conference Bridge Configuration Checklist, page 24-11
- Where to Find More Information, page 24-11

Understanding Conference Devices

Cisco Unified CallManager supports multiple conference devices to distribute the load of mixing audio between the endpoints involved in a conference. A component of Cisco Unified CallManager called Media Resource Manager (MRM) locates and assigns resources throughout a cluster. The MRM resides on every Cisco Unified CallManager server and communicates with MRMs on other Cisco Unified CallManager servers.

Cisco Unified CallManager supports hardware and software conference devices; both hardware and software conference bridges can be active at the same time.

For conferencing, you must determine the total number of concurrent users (or audio streams) that are required at any given time. (An audio stream is a two-way audio path in a conference that supports one stream for each endpoint/participant.) Then, if you plan to use a software conference device, you create and configure the device to support the calculated number of streams (see the "Software Conference Devices" section on page 24-3 for information about calculating number of streams). You cannot configure the number of streams for hardware conference bridges. One large conference, or several small conferences, can use these audio streams.

Caution Although a single software conference device can run on the same server as the Cisco Unified CallManager service, Cisco strongly recommends against this configuration. Running a conference device on the same server as the Cisco CallManager service may adversely affect performance on the Cisco Unified CallManager.

For more information on hardware and software conference devices, see the following sections:

- Router-Based Conference Capability, page 24-2
- Software Conference Devices, page 24-3
- Video Conference Devices, page 24-3
- Cisco Conference Devices (WS-SVC-CMM), page 24-3
- MTP WS-X6608 DSP Service Card, page 24-4
- Annunciator Support for Conference Bridges, page 24-4
- Conference Bridge Types in Cisco Unified CallManager Administration, page 24-4

Router-Based Conference Capability

The Cisco 1700, Cisco 2600, Cisco 2600XM, Cisco 2800, Cisco 3600, Cisco 3700, and Cisco 3800 series voice gateway routers provide conferencing capabilities for Cisco Unified CallManager. These routers provide conferencing with two features:

- Cisco Conferencing and Transcoding for Voice Gateway Routers by using the NM-HDV or NM-HDV-FARM network modules. This feature supports up to six parties in a conference. (Choose the Cisco IOS Conference Bridge from the Conference Bridge Configuration window in Cisco Unified CallManager Administration to support this feature.)
- Cisco Enhanced Conferencing and Transcoding for Voice Gateway Routers by using the Cisco Packet Voice/Fax Digital Signal Processor Modules (PVDM2) on the Cisco 2800 and 3800 series voice gateway routers or using the NM-HD or NM-HDV2 network modules. This feature supports eight parties in a conference. (Choose the Cisco IOS Enhanced Conference Bridge from the Conference Bridge Configuration window in Cisco Unified CallManager Administration to support this feature.)

For more information about these conferencing routers, refer to the IOS router documentation provided with your router.

Router-enabled conferencing provides the ability to support voice conferences in hardware. Digital Signal Processors (DSPs) convert multiple Voice over IP Media Streams into TDM streams that are mixed into a single conference call stream. The DSPs support both meet-me and ad hoc conferences by Cisco Unified CallManager.

The Cisco routers that support conferencing have the following codecs:

- G.711 a/u-law
- G.729, G.729a, G.729b, G.729ab
- GSM FR, GSM EFR (only supports Cisco Enhanced Conferencing and Transcoding for Voice Gateway Routers feature)

Software Conference Devices

For software conference devices, you can adjust the number of streams because software conference devices support a variable number of audio streams. You can configure a software conference device and choose the number of full-duplex audio streams that the device supports. To calculate the total number of conferences that a device supports, divide the number of audio streams by three (the minimum number of participants in a conference). The maximum number of audio streams equals 128. For more information on software conference devices, see the "Conference Bridge Types in Cisco Unified CallManager Administration" section on page 24-4.

Video Conference Devices

The Cisco video conference bridge, a dual multimedia bridge, provides video conferencing. Cisco Unified CallManager controls this conference bridge type upon appropriate configuration. The Cisco video conference bridge provides audio and video conferencing functions for Cisco IP video phones, H.323 endpoints, and audio-only Cisco IP Phones. Administrators can partition the resources of the Cisco video conference bridge between the video telephony network and the H.323/SIP network. The Cisco video conference bridge supports the H.261, H.263, and H.264 codecs for video.

To configure this type of conference device, the user chooses the Cisco Video Conference Bridge (IPVC-35xx) conference bridge type in Cisco Unified CallManager Administration.

To ensure that only a video conference bridge gets used when a user wants to hold a video conference, add the video conference bridge to a media resource group. Add the media resource group to a media resource group list and assign the media resource group list to the device or device pool that will use the video conference bridge. Refer to the Conference Bridge Configuration, Media Resource Group Configuration, Media Resource Group List Configuration, and Device Pool Configuration sections of the *Cisco Unified CallManager Administration Guide* for details. Refer to the *Cisco Unified Videoconferencing MCU 3511 and Cisco Unified Videoconferencing MCU 3540 Module Administrator Guide* for more information about the Cisco video conference bridge.

Cisco Conference Devices (WS-SVC-CMM)

Applications can control a Cisco Unified CallManager Conference Bridge (WS-SVC-CMM). For more information on Cisco Conference Devices (WS-SVC-CMM), see the "Conference Bridge Types in Cisco Unified CallManager Administration" section on page 24-4.

To configure this type of conference device, the user chooses the Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) conference bridge type in Cisco Unified CallManager Administration.

MTP WS-X6608 DSP Service Card

Because hardware conference devices are fixed at 32 full-duplex streams per WS-X6608 port, hardware conference devices support 32 divided by three (32/3), or 10, conferences. Users cannot change this value.

Caution Full-duplex streams per WS-X6608 port cannot exceed the maximum limit of 32.

Annunciator Support for Conference Bridges

Cisco Unified CallManager provides annunciator resource support to a conference bridge under the following circumstances:

- If the media resource group list that contains the annunciator is assigned to the device pool where the conference bridge exists.
- If the annunciator is configured as the default media resource, which makes it available to all devices in the cluster.

Cisco Unified CallManager does not provide annunciator resource support for a conference bridge if the media resource group list is assigned directly to the device that controls the conference.

Conference Bridge Types in Cisco Unified CallManager Administration

The conference bridge types in Table 24-1 exist in Cisco Unified CallManager Administration.

Table 24-1 Conference Bridge Types

Conference Bridge Type	Description
Cisco Unified CallManager Conference Bridge Hardware (WS-6608-T1 or WS-6608-E1)	This type supports the Cisco Catalyst 4000 and 6000 Voice Gateway Modules and the following number of conference sessions. **Cisco Catalyst 6000** • G.711 or G.729a conference—32 participants per port; six participants maximum per conference; 256 total participants per module; 10 bridges with three participants • GSM—24 participants per port; six participants maximum per conference; 192 total participants per module **Cisco Catalyst 4000** • G.711 conference only—24 conference participants; maximum of four conferences with six participants each

Table 24-1 Conference Bridge Types (continued)

Conference Bridge Type	Description
Cisco Unified CallManager Conference Bridge Software	Software conference devices support G.711 codecs by default. The maximum number of audio streams for this type equals 128. With 128 streams, a software conference media resource can handle 128 users in a single conference, or the software conference media resource can handle up to 42 conferencing resources with three users per conference. ⚠ **Caution** If the Cisco IP Voice Media Streaming Application service runs on the same server as the Cisco CallManager service, a software conference should not exceed the maximum limit of 48 participants.
Cisco IOS Conferencing and Transcoding for Voice Gateway Routers	• Uses the NM-HDV or NM-HDV-FARM network modules. • G.711 a/u-law, G.729, G.729a, G.729b, and G.729ab participants joined in a single conference • Up to six parties joined in a single conference call Cisco Unified CallManager assigns conference resources to calls on a dynamic basis. In a Cisco Unified CallManager network that includes both Cisco IOS Conferencing and Cisco IOS Enhanced Conferencing, set the Cisco CallManager service parameters, Maximum Ad hoc Conference and the Maximum MeetMe Conference Unicast, to six conference participants. For more information about Cisco IOS Conferencing and Transcoding for Voice Gateway Routers, see the IOS documentation that you received with this product.
Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Routers	• Uses the onboard Cisco Packet Voice/Fax Digital Signal Processor Modules (PVDM2) on the Cisco 2800 and 3800 series voice gateway routers or uses the NM-HD or NM-HDV2 network modules. • G.711 a-law/mu-law, G.729, G.729a, G.729b, G.729ab, GSM FR, and GSM EFR participants joined in a single conference • Up to eight parties joined in a single call. **Tip** In Cisco Unified CallManager Administration, ensure that you enter the same conference bridge name that exists in the gateway Command Line Interface. Cisco Unified CallManager assigns conference resources to calls on a dynamic basis. In a Cisco Unified CallManager network that includes both Cisco IOS Conferencing and Cisco IOS Enhanced Conferencing, set the Cisco CallManager service parameters, Maximum Ad hoc Conference and the Maximum MeetMe Conference Unicast, to six conference participants. For more information about Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Routers, see the IOS documentation that you received with this product.

Table 24-1 Conference Bridge Types (continued)

Conference Bridge Type	Description
Cisco Video Conference Bridge (IPVC-35xx)	This conference bridge type specifies a dual multimedia bridge that provides video conferencing. The Cisco video conference bridge provides audio and video conferencing functions for Cisco IP video phones, H.323 endpoints, and audio-only Cisco IP Phones.
Cisco Unified CallManager Conference Bridge (WS-SVC-CMM)	This conference bridge type supports the Cisco Catalyst 6500 series and Cisco 7600 series Communication Media Module (CMM). This conference bridge type supports up to eight parties per conference and up to 64 conferences per port adapter. This conference bridge type supports the following codecs: G.711 mu-law, G.711 a-law, G.729 annex A and annex B, and G.723.1. This conference bridge type supports ad hoc conferencing.

Using Different Conference Types: Meet Me and Ad Hoc

Cisco Unified CallManager supports both meet-me conferences and ad hoc conferences. Meet-me conferences allow users to dial in to a conference. Ad hoc conferences allow the conference controller to let only certain participants into the conference.

Initiating an Ad Hoc Conference

Initiate ad hoc conferences in the following ways:

- When in an existing call, press the Conference softkey, dial another participant, and conference additional participants.
- Join established calls by using the Select and Join softkeys.
- Conference established call by using the cBarge softkey.

Using Conference Softkey for Ad Hoc Conference

The conference controller controls ad hoc conferences. When you initiate an ad hoc conference, Cisco Unified CallManager considers you the conference controller. In an ad hoc conference, only a conference controller can add and remove participants from a conference. If sufficient streams are available on the conference device, the conference controller can add up to the maximum number of participants that is specified for ad hoc conferences to the conference. (Configure the maximum number of participants for an ad hoc conference in Cisco Unified CallManager Administration, Cisco CallManager Service Parameters Configuration by using the Maximum Ad Hoc Conference service parameter setting.) Cisco Unified CallManager supports multiple, concurrent ad hoc conferences on each line appearance of a device.

When the conference controller initiates a conference call, Cisco Unified CallManager places the current call on hold, flashes the conference lamp (if applicable), and provides dial tone to the user. At the dial tone, the conference controller dials the next conference participant and presses the Conference softkey to complete the conference. Cisco Unified CallManager then connects the conference controller, the first participant, and the new conference participant to a conference bridge. Each participating Cisco IP Phone display reflects the connection to the conference.

The conference controller can view the list of conference participants by pressing the Conference List (ConfList) softkey (any participant can view the list of participants) and can drop the last conference participant from the conference by pressing the Remove Last Conference Party (RmLstC) softkey on the Cisco Unified IP Phone. If a conference participant transfers the conference to another party, the transferred party becomes the last conference participant in the conference. If a conference participant parks the conference, the participant becomes the last party in the conference when the participant picks up the conference. When only two participants remain in the conference, Cisco Unified CallManager terminates the conference, and the two remaining participants reconnect directly as a point-to-point call.

Participants can leave a conference by simply hanging up. A conference continues even when the conference controller hangs up, although the remaining conference participants cannot add new participants to the conference. See the "Ad Hoc Conference Settings" section on page 24-7 for more information about configuring ad hoc conferences and their behavior.

Conference by Using Join Softkey

The user initiates an ad hoc conference by using the Select and Join softkeys. During an established call, the user chooses conference participants by pressing the Select softkey and then presses the Join softkey, making it an ad hoc conference. Up to 15 established calls can be added to the ad hoc conference, for a total of 16 participants. Cisco Unified CallManager treats the ad hoc conference the same way as one that is established by using the Conference softkey method.

Conference by Using cBarge Softkey

You can initiate a conference by pressing the cBarge softkey. 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. The call information for all parties gets changed to Conference.

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, leaving only two parties in the conference, the remaining two parties get reconnected as a point-to-point call, which releases the shared conference resource.

For more information about shared conferences using cBarge, see Barge and Privacy in the *Cisco Unified CallManager Features and Services Guide*.

Ad Hoc Conference Settings

Cisco Unified CallManager Administration provides the clusterwide service parameter, Drop Ad Hoc Conference, to allow the prevention of toll fraud (where an internal conference controller disconnects from the conference while outside callers remain connected). The service parameter settings specify conditions under which an ad hoc conference gets dropped.

Note The Drop Ad Hoc Conference service parameter works differently for conference calls that are initiated from a Cisco SIP IP Phone 7940 or 7960 or a third-party SIP phone. See the "Ad Hoc Conference Settings Restrictions for SIP Phones" section on page 24-8.

To configure the value of the service parameter, perform the following procedure:

Procedure

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

Step 2 From the Server drop-down list box, choose a server in the cluster.

Step 3 From the Service drop-down list box, choose Cisco CallManager.

Step 4 From the Drop Ad Hoc Conference drop-down list box, which is listed in the Clusterwide Parameters (Features - General) area of the window, choose one of the following options:

- **Never**—The conference is not dropped. (This is the default option.)
- **When No OnNet Parties Remain in the Conference**—The system drops the active conference when the last on-network party in the conference hangs up or drops out of the conference. Cisco Unified CallManager releases all resources that are assigned to the conference.

  For more information about OnNet and OffNet, refer to the Understanding Cisco Unified CallManager Voice Gateways, Understanding Cisco Unified CallManager Trunk Types, and Understanding Route Plans chapters in the *Cisco Unified CallManager System Guide*.
- **When Conference Controller Leaves**—The active conference terminates when the primary controller (conference creator) hangs up. Cisco Unified CallManager releases all resources that are assigned to the conference.

Note If the conference controller transfers, parks, or redirects the conference to another party, the party that retrieves the call acts as the virtual controller for the conference. A virtual controller cannot add new parties to the conference nor remove any party that was added to the conference, but a virtual controller can transfer, park, or redirect the conference to another party, who would, in turn, become the virtual controller of the conference. When this virtual controller hangs up the call, the conference ends.

Step 5 Click **Save**.

Note Cisco Unified CallManager does not support multiple options; that is, all conferences will support the same functionality depending on the option that you choose.

Ad Hoc Conference Settings Restrictions for SIP Phones

Conference calls that are initiated by a SIP phone (Cisco SIP IP Phone 7940/60 and third-party SIP phones) have limitations when using ad-hoc conferencing. Cisco Unified CallManager does not see this type of call as a conference call, it sees them as individual calls; therefore, the following restrictions apply:

- The SIP phone display differs from the SCCP phone display; for example, SCCP phones display the call as a conference call whereas SIP phones display the calls that are conferenced as individual calls (with a conference icon next to each call).
- Conference list (ConfList) is not available
- Remove last conference participant (RmLstC) is not available
- Because Cisco Unified CallManager does not recognize the SIP phone-initiated conference call as a conference, the Drop Ad Hoc Conference service parameter settings do not apply.
- The SIP Profile parameter, Conference Join Enabled, controls SIP phone behavior when the conference controller exits a locally hosted conference. If the Conference Join Enabled check box is unchecked, all legs are disconnected when the conference controller exits the ad hoc conference call. If the Conference Join Enabled check box is checked, the remaining two parties stay connected.

- To achieve the same level of control that the Drop Ad Hoc Conference parameter settings provides for SCCP phone-initiated conference calls, the administrator can use a combination of the Conference Join Enabled SIP profile parameter and the Block OffNet to OffNet Transfer service parameter for conferences that are initiated on the SIP phone. (Because the SIP phone performs a transfer when it drops out of the conference call, the Block OffNet to OffNet Transfer can prevent toll fraud by not allowing two offnet phones to remain in the call.)

Ad Hoc Conference Limitations

Cisco Unified CallManager supports a maximum of 100 simultaneous ad hoc conferences for each Cisco Unified CallManager server.

Initiating a Meet-Me Conference

Meet-me conferences require that a range of directory numbers be allocated for exclusive use of the conference. When a meet-me conference is set up, the conference controller chooses a directory number and advertises it to members of the group. The users call the directory number to join the conference. Anyone who calls the directory number while the conference is active joins the conference. (This situation applies only when the maximum number of participants that is specified for that conference type has not been exceeded and when sufficient streams are available on the conference device.)

When you initiate a meet-me conference by pressing Meet-Me on the phone, Cisco Unified CallManager considers you the conference controller. The conference controller provides the directory number for the conference to all attendees, who can then dial that directory number to join the conference. If other participants in a meet-me conference press Meet-Me and the same directory number for the conference bridge, the Cisco Unified CallManager ignores the signals.

The conference controller chooses a directory number from the range that is specified for the Meet-Me Number/Pattern. The Cisco Unified CallManager Administrator provides the meet-me conference directory number range to users, so they can access the feature.

A meet-me conference continues even if the conference controller hangs up.

Meet-Me Conference Limitations

Cisco Unified CallManager supports a maximum of 100 simultaneous meet-me conferences for each Cisco Unified CallManager server.

Dependency Records

To find out which media resource groups are associated with a conference bridge, click the Dependency Records link that is provided on the Cisco Unified CallManager Administration Conference Bridge Configuration window. The Dependency Records Summary window displays information about media resource groups that are using the conference bridge. To find out more information about the media resource group, click the media resource group, 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 Unified CallManager Administration Guide*.

Conference Bridge Performance Monitoring and Troubleshooting

The Real Time Monitoring Tool counters for conference bridges allow you to monitor the number of conference bridges that are currently registered with the Cisco Unified CallManager but are not currently in use, the number of conferences that are currently in use, the number of times that a conference completed, and the number of times that a conference was requested for a call but no resources were available.

For more information about Real Time Monitoring Tool counters, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Cisco Unified CallManager writes all errors for conference bridges to the Local SysLog Viewer in the Real Time Monitoring Tool. In Cisco Unified CallManager Serviceability, you can set traces for the Cisco IP Voice Media Streaming Application service (using Trace Configuration); to troubleshoot most issues, you must choose the Significant or Detailed option for the service, not the Error option. After you troubleshoot the issue, change the Debug Trace Level back to the Error option.

Cisco Unified CallManager generates registration and connection alarms for conference bridges in Cisco Unified CallManager Serviceability. For more information on alarms, refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System Guide*.

If you need technical assistance, locate conference bridge logs from

/var/log/active/cm/trace/cms/sdi/cms* and /var/log/active/cm/trace/ccm before you contact your Cisco Partner or the Cisco Technical Assistance Center (TAC).

Use the following commands to access the logs:

```
file list activelog cm/trace/cms/sdi/*.txt

file get activelog cm/trace/cms/sdi/*.txt

file view activelog cm/trace/cms/sdi/cms00000000.txt

file tail activelog cm/trace/cms/sdi/cms00000000.txt
```

Conference Bridge Configuration Checklist

Table 24-2 provides a checklist to configure conference bridge.

Table 24-2 Conference Bridge Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure the hardware or software conference bridge(s).	Adding a Hardware Conference Device, *Cisco Unified CallManager Administration Guide* Adding a Cisco IOS Conference Bridge Device, *Cisco Unified CallManager Administration Guide* Adding a Cisco Video Conference Bridge Device, *Cisco Unified CallManager Administration Guide* Adding a Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) Device, *Cisco Unified CallManager Administration Guide* Software Conference Bridge Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 2	Configure the Meet-Me Number/Pattern.	Meet-Me Number/Pattern Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Add a Conference button for ad hoc or Meet Me Conference button for the meet-me conference to the phone templates, if needed. You only need to do this for Cisco IP Phone models 12 SP, 12 SP+, and 30 VIP.	Deleting a Phone Button Template, *Cisco Unified CallManager Administration Guide*
Step 4	If users will use the Join, ConfList, and RmLstC softkeys, modify either the Standard Feature or Standard User softkey template and assign the modified softkey template to the user device.	Modifying Softkey Templates, *Cisco Unified CallManager Administration Guide*
Step 5	Configure the ad hoc conference settings.	Initiating an Ad Hoc Conference, page 24-6.
Step 6	Notify users that the Conference Bridge feature is available. If applicable, notify users of the meet-me conference number range.	Refer to the phone documentation for instructions on how users access conference bridge features on their Cisco Unified IP Phone.

Where to Find More Information

Related Topics

- Server Configuration, *Cisco Unified CallManager Administration Guide*
- Phone Button Template Configuration, *Cisco Unified CallManager Administration Guide*

- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*
- Partition Configuration, *Cisco Unified CallManager Administration Guide*
- Conference Bridge Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco DSP Resources for Transcoding, Conferencing, and MTP, page 28-1

Additional Cisco Documentation

- *Cisco IP Phone Administration Guide for Cisco Unified CallManager*
- Cisco IP Phone user documentation and release notes (all models)
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified Videoconferencing 3511 MCU and Cisco Unified Videoconferencing 3540 MCU Module Administrator Guide*

CHAPTER 25

Transcoders

The Media Resource Manager (MRM) provides resource reservation of transcoders within a Cisco Unified CallManager cluster. Cisco Unified CallManager supports simultaneous registration of both the MTP and transcoder and concurrent MTP and transcoder functionality within a single call.

This section covers the following topics:

- Understanding Transcoders, page 25-1
- Managing Transcoders with the Media Resource Manager, page 25-2
- Using Transcoders as MTPs, page 25-2
- Transcoder Types in Cisco Unified CallManager Administration, page 25-2
- Transcoder Failover and Fallback, page 25-3
- Dependency Records, page 25-4
- Transcoder Performance Monitoring and Troubleshooting, page 25-4
- Transcoder Configuration Checklist, page 25-5
- Where to Find More Information, page 25-5

Understanding Transcoders

A transcoder takes the stream of one codec and transcodes (converts) it from one compression type to another compression type. For example, it could take a stream from a G.711 codec and transcode (convert) it in real time to a G.729 stream. In addition, a transcoder provides MTP capabilities and may be used to enable supplementary services for H.323 endpoints when required.

The Cisco Unified CallManager invokes a transcoder on behalf of endpoint devices when the two devices use different voice codecs and would normally not be able to communicate. When inserted into a call, the transcoder converts the data streams between the two incompatible codecs to enable communications between them.The transcoder remains invisible to either the user or the endpoints that are involved in a call.

A transcoder provides a designated number of streaming mechanisms, each of which can transcode data streams between different codecs and enable supplementary services, if required, for calls to H.323 endpoints.

For more information on transcoders, see the following sections:

- Using Transcoders as MTPs, page 25-2
- Transcoder Types in Cisco Unified CallManager Administration, page 25-2

Managing Transcoders with the Media Resource Manager

All Cisco Unified CallManagers within a cluster can access transcoders through the Media Resource Manager (MRM). The MRM manages access to transcoders.

The MRM makes use of Cisco Unified CallManager media resource groups and media resource group lists. The media resource group list allows transcoders to communicate with other devices in the assigned media resource group, which in turn, provides management of resources within a cluster.

A transcoder control process gets created for each transcoder device that is defined in the database. The MRM keeps track of the transcoder resources and advertises their availability throughout the cluster.

Using Transcoders as MTPs

The CAT6000 WS-X6608-T1/E1 transcoder port resources also support MTP functionality to enable supplementary services for H.323 endpoints if no software MTP is available within the Cisco Unified CallManager cluster. In this capacity, when the Cisco Unified CallManager determines that an endpoint in a call requires an MTP, it allocates a transcoder resource and inserts it into the call, where it acts like an MTP transcoder.

Cisco Unified CallManager supports MTP and transcoding functionality simultaneously. For example, if a call originates from a Cisco IP Phone (located in the G723 region) to NetMeeting (located in the G711 region), one transcoder resource supports MTP and transcoding functionality simultaneously.

If a software MTP/transcoder resource is not available when it is needed, the call connects without using a transcoder resource, and that call does not have supplementary services. If hardware transcoder functionality is required (to convert one codec to another) and a transcoder is not available, the call will fail.

Transcoder Types in Cisco Unified CallManager Administration

You can choose the transcoder types in Table 25-1 from Cisco Unified CallManager Administration.

Table 25-1 Transcoder Types

Transcoder Type	Description
Cisco Media Termination Point Hardware	This type, which supports the Cisco Catalyst 4000 WS-X4604-GWY and the Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1, provides the following number of transcoding sessions: **For the Cisco Catalyst 4000 WS-X4604-GWY** • For transcoding to G.711—16 MTP transcoding sessions **For the Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1** • For transcoding from G.723 to G.711/For transcoding from G.729 to G.711—24 MTP transcoding sessions per physical port; 192 sessions per module

Table 25-1 Transcoder Types (continued)

Transcoder Type	Description
Cisco IOS Media Termination Point	This type, which supports the Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745, Cisco 3660, Cisco 3640, Cisco 3620, Cisco 2600, and Cisco VG200 gateways, provides the following number of transcoding sessions: **Per NM-HDV** • Transcoding from G.711 to G.729—60 • Transcoding from G.711 to GSM FR/GSM EFR— 45
Cisco IOS Enhanced Media Termination Point	**Per NM-HD** This type, which supports Cisco 2600XM, Cisco 2691, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco 3660 Access Routers, provides the following number of transcoding sessions: • Transcoding for G.711 to G.729a/G.729ab/GSMFR—24 • Transcoding for G.711 to G.729/G.729b/GSM EFR—18 **Per NM-HDV2** This type, which supports Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745, and Cisco 3660 Access Routers, provides the following number of transcoding sessions: • Transcoding for G.711 to G.729a/G.729ab/GSMFR—128 • Transcoding for G.711 to G.729/G.729b/GSM EFR—96
Cisco Media Termination Point (WS-SVC-CMM)	This type provides 64 transcoding sessions per daughter card that is populated: 64 transcoding sessions with one daughter card, 128 transcoding sessions with two daughter cards, 192 transcoding sessions with three daughter cards, and 256 transcoding sessions with four daughter cards (maximum). This type provides transcoding between any combination of the following codecs: • G.711 a-law and G.711 mu-law • G.729 annex A and annex B • G.723.1 • GSM (FR) • GSM (EFR)

Transcoder Failover and Fallback

This section describes how transcoder devices failover and fallback when the Cisco Unified CallManager to which they are registered becomes unreachable. The section also explains conditions that can affect calls that are associated with a transcoder device, such as transcoder 1 reset or restart.

Related Topics

- Active Cisco Unified CallManager Becomes Inactive, page 25-4
- Resetting Registered Transcoder Devices, page 25-4

Active Cisco Unified CallManager Becomes Inactive

The following items describe the MTP device recovery methods when the MTP is registered to a Cisco Unified CallManager that goes inactive:

- If the primary Cisco Unified CallManager fails, the transcoder attempts to register with the next available Cisco Unified CallManager in the Cisco Unified CallManager Group that is specified for the device pool to which the transcoder belongs.
- The transcoder device reregisters with the primary Cisco Unified CallManager as soon as Cisco Unified CallManager becomes available.
- A transcoder device unregisters with a Cisco Unified CallManager that becomes unreachable. The calls that were on that Cisco Unified CallManager will register with the next Cisco Unified CallManager in the list.
- If a transcoder attempts to register with a new Cisco Unified CallManager and the register acknowledgment is never received, the transcoder registers with the next Cisco Unified CallManager.

Resetting Registered Transcoder Devices

The transcoder devices will unregister and then disconnect after a hard or soft reset. After the reset completes, the devices reregister with the primary Cisco Unified CallManager.

Dependency Records

To find out which media resources are associated with a transcoder, choose Dependency Records from the Related Links drop-down list box from the Cisco Unified CallManager Administration Transcoder Configuration window. Click **Go**. The Dependency Records Summary window displays information about media resource groups that are using the transcoder. To find out more information about the media resource group, click the media resource group, 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 Unified CallManager Administration Guide*.

Transcoder Performance Monitoring and Troubleshooting

Microsoft Performance Monitor counters for transcoders allow you to monitor the number of transcoders that are currently in use, the number of transcoders that are currently registered with the Cisco Unified CallManager but are not currently in use, and the number of times that a transcoder was requested for a call, but no resources were available.

For more information about performance monitor counters, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Cisco Unified CallManager writes all errors for the transcoder to the Event Viewer. In Cisco Unified CallManager Serviceability, you can set traces for the Cisco IP Voice Media Streaming Application service; to troubleshoot most issues, you must choose the Significant or Detail option for the service, not the Error option. After you troubleshoot the issue, change the service option back to the Error option.

For more information about the Cisco IP Voice Media Streaming Application service, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Cisco Unified CallManager generates registration and connection alarms for transcoder in Cisco Unified CallManager Serviceability. For more information on alarms, refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System Guide*.

Transcoder Configuration Checklist

Table 25-2 provides a checklist to configure transcoders.

Table 25-2 Transcoder Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Determine the number of transcoder resources that are needed and the number of transcoder devices that are needed to provide these resources.	Transcoder Configuration, *Cisco Unified CallManager Administration Guide*
Step 2	Add and configure the transcoders.	Transcoder Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Add the new transcoders to the appropriate media resource groups.	Media Resource Management, page 22-1 Media Resource Group Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 4	Restart the transcoder device.	Resetting a Transcoder, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topics

- Media Resource Management, page 22-1
- Media Termination Points, page 27-1
- Cisco DSP Resources for Transcoding, Conferencing, and MTP, page 28-1
- Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide*
- Media Resource Group Configuration Settings, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design Guide*

CHAPTER 26

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.

For information and configuration procedures for Music on Hold, refer to the Music On Hold chapter in the *Cisco Unified CallManager Features and Services Guide*.

CHAPTER 27

Media Termination Points

A Media Termination Point (MTP) software device allows Cisco Unified CallManager to relay calls that are routed through SIP or H.323 endpoints or gateways.

This section covers the following topics:

- Understanding Media Termination Points, page 27-1
- Managing MTPs with the Media Resource Manager, page 27-2
- MTP Types in Cisco Unified CallManager Administration, page 27-3
- Planning Your Software MTP Configuration, page 27-3
- MTP System Requirements and Limitations, page 27-5
- MTP Failover and Fallback, page 27-5
- Dependency Records, page 27-6
- Software MTP Performance Monitoring and Troubleshooting, page 27-6
- Software MTP Configuration Checklist, page 27-7
- Where to Find More Information, page 27-7

Note For information on hardware MTP, which act as transcoders, see the "Transcoders" section on page 25-1.

Understanding Media Termination Points

Media Termination Points extend supplementary services, such as call hold, call transfer, call park, and conferencing, that are otherwise not available when a call is routed to an H.323 endpoint. Some H.323 gateways may require that calls use an MTP to enable supplementary call services, but normally, Cisco IOS gateways do not.

The Cisco IP Voice Media Streaming Application MTP accepts two full-duplex G.711 Coder-Decoder (CODEC) stream connections. MTPs bridge the media streams between two connections. The streaming data that is received from the input stream on one connection passes to the output stream on the other connection and vice versa. In addition, the MTP trancodes a-law to mu-law (and vice versa) and adjusts packet sizes as required by the two connections.

Each MTP belongs to a device pool, which specifies, in priority order, the list of Cisco Unified CallManagers to which the devices that are members of the device pool should attempt to register. This list represents a Cisco Unified CallManager group. The first Cisco Unified CallManager in the list specifies a device primary Cisco Unified CallManager.

An MTP device always registers with its primary Cisco Unified CallManager if that Cisco Unified CallManager is available and informs the Cisco Unified CallManager about how many MTP resources it supports. The Cisco Unified CallManager controls MTP resources. You can register multiple MTPs with the same Cisco Unified CallManager. When more than one MTP is registered with a given Cisco Unified CallManager, that Cisco Unified CallManager controls the set of resources for each MTP. You can also distribute the MTPs across a networked system as desired.

For example, consider MTP server 1 as configured for 48 MTP resources, and the MTP server 2 as configured for 24 resources. If both MTPs register with the same Cisco Unified CallManager, that Cisco Unified CallManager maintains both sets of resources for a total of 72 registered MTP resources.

When the Cisco Unified CallManager determines that a call endpoint requires an MTP, it allocates an MTP resource from the MTP that has the least active streams. That MTP resource gets inserted into the call on behalf of the endpoint. MTP resource use remains invisible to both the users of the system and to the endpoint on whose behalf it was inserted. If an MTP resource is not available when it is needed, the call connects without using an MTP resource, and that call does not have supplementary services.

Make sure that the Cisco IP Voice Media Streaming application is activated and running on the server on which the MTP device is configured.

The Cisco IP Voice Media Streaming application, which is common to the MTP, Conference Bridge, annunciator, and Music On Hold applications, runs as a Cisco Unified CallManager service.

You can add an MTP device in two ways:

- You automatically add an MTP device when you activate the Cisco IP Voice Media Streaming Application service from Cisco Unified CallManager Serviceability.
- You can manually install the Cisco IP Voice Media Streaming Application on a networked server and configure an MTP device on that server through Cisco Unified CallManager Administration.

SIP and MTP

Cisco Unified CallManager requires an RFC 2833 DTMF-compliant MTP device to make SIP calls. The current standard for SIP uses inband payload types to indicate DTMF tones, and Cisco Unified Communications components such as SCCP IP phones support only out-of-band payload types. Thus, an RFC 2833-compliant MTP device monitors for payload type and acts as a translator between inband and out-of-band payload types.

With the MTP device, any service that requires a media change (such as call hold) happens transparently. No need exists to send any media update signal to the SIP proxy server.

Managing MTPs with the Media Resource Manager

The Media Resource Manager (MRM), a software component in the Cisco Unified CallManager system, primarily functions for resource registration and resource reservation. Each MTP device that is defined in the database registers with the MRM. The MRM keeps track of the total available MTP devices in the system and of which devices have available resources.

During resource reservation, the MRM determines the number of resources, identifies the media resource type (in this case, the MTP), and the location of the registered MTP device. The MRM updates its shared resource table with the registration information and propagates the registered information to the other Cisco Unified CallManagers within the cluster.

The MRM enhances the Cisco Unified CallManager MTP, Music On Hold, Conference Bridge, and Transcoder devices by distributing the resources throughout the Cisco Unified CallManager cluster, which makes the features more efficient and economical.

MRM also supports the coexistence of an MTP and transcoder within a Cisco Unified CallManager.

MTP Types in Cisco Unified CallManager Administration

The media termination point types in Table 27-1 exist in Cisco Unified CallManager Administration.

Table 27-1 Media Termination Point Types

MTP Type	Description
Cisco IOS Enhanced Software Media Termination Point	This type supports Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745, and Cisco 3660 Access Routers and the following MTP cases: • For software-only implementation that does not use DSP but has the same packetization time for devices that support G.711 to G.711 or G.729 to G.729 codecs, this implementation can support up to 500 sessions per gateway. • For a hardware-only implementation with DSP for devices that use G.711 codec only, 200 sessions can occur per NM-HDV2 and 48 sessions can occur per NM-HD. **Tip** Cisco IOS Software Enhanced Media Termination Point does not support RFC 2833 (DTMF relay). This type can support Network Address Translation in a service provider environment to hide the private address. In Cisco Unified CallManager Administration, ensure that you enter the same MTP name that exists in the gateway Command Line Interface (CLI).
Cisco Media Termination Point Software	A single MTP provides a default of 48 MTP (user configurable) resources, depending on the speed of the network and the network interface card (NIC). For example, a 100-MB Network/NIC card can support 48 MTP resources, while a 10-MB NIC card cannot. For a 10-MB Network/NIC card, approximately 24 MTP resources can be provided; however, the exact number of MTP resources that are available depends on the amount of resources that other applications on that PC are consuming, the speed of the processor, network loading, and various other factors.

Planning Your Software MTP Configuration

Provisioning represents a crucial aspect that needs consideration when MTP resources are deployed. Provisioning requires attentive analysis of the call load patterns and the network topology.

Consider the following information when you are planning your MTP configuration:

- An improper setting can result in undesirable performance if the workload is too high.
- A single MTP provides a default of 48 MTP (user configurable) resources, depending on the speed of the network and the network interface card (NIC). For example, a 100-MB Network/NIC card can support 48 MTP resources, while a 10-MB NIC card cannot.
- For a 10-MB Network/NIC card, approximately 24 MTP resources can be provided; however, the exact number of MTP resources that are available depends on the amount of resources that other applications on that PC are consuming, the speed of the processor, network loading, and various other factors.

  Consider the following formula to determine the approximate number of MTPs that are needed for your system, assuming that your server can handle 48 MTP resources (you can substitute 48 for the correct number of MTP resources that your system supports):

  A number divided by 48 = number of MTP applications that are needed ($n/48$ = number of MTP applications).

  where:

  n represents the number of devices that require MTP support for H.323 and SIP calls.

  If a remainder exists, add another server with Cisco IP Voice Streaming Application server with MTP.
- If one H.323 or SIP endpoint requires an MTP, it consumes one MTP resource. Depending on the originating and terminating device type, a given call might consume more than one MTP resource. The MTP resources that are assigned to the call get released when the call terminates.
- Use Performance Monitor to monitor the usage of MTP resources. The Performance Monitor counter, Media TermPoints Out of Resources, increments for each H.323 or SIP call that connects without an MTP resource when one was required. This number can assist you in determining how many MTP resources are required for your callers and whether you have adequate coverage.
- Identical system requirements apply for the Cisco IP Voice Media Streaming Application and MTP and the Cisco Unified CallManager system.
- Cisco Unified CallManager requires an RFC 2833 DTMF-compliant MTP device to make SIP calls.

Software MTP Device Characteristics

The Full Streaming Endpoint Duplex Count, a number of MTP resources that a specific MTP supports, represents a device characteristic that is specific to MTP device configuration. Refer to the "Related Topics" section in the *Cisco Unified CallManager Administration Guide* for a detailed description of all MTP device settings.

Avoiding Call Failure/User Alert

To prevent call failure or user alert, avoid the following conditions:

- Although the Cisco IP Voice Media Streaming Application service can run on the same PC as the Cisco Unified CallManager, we strongly recommend against this arrangement. If the Cisco IP Voice Media Streaming Application is running on the same PC as the Cisco Unified CallManager, it can adversely affect the performance of the Cisco Unified CallManager.

- When you configure the MTP, a prompt asks you to reset MTP before any changes can take effect. This action does not result in disconnection of any calls that are connected to MTP resources. If you choose **Reset**, as soon as the MTP has no active calls, the changes take effect.

Note When you make updates to the MTP and you choose **Restart**, all calls that are connected to the MTP get dropped.

MTP System Requirements and Limitations

The following system requirements and limitations apply to software MTP devices:

- You can activate only one Cisco IP Voice Streaming Application per server. To provide more MTP resources, you can activate the Cisco IP Voice Streaming application on additional networked Windows NT servers.
- Each MTP can register with only one Cisco Unified CallManager at a time. The system may have multiple MTPs, each of which may be registered to one Cisco Unified CallManager, depending on how your system is configured.
- Cisco strongly recommends that you do not activate the Cisco IP Voice Streaming Media Application on a Cisco Unified CallManager with a high call-processing load because it can adversely affect the performance of the Cisco Unified CallManager.
- Up to 128 half-duplex configurable streams must exist.
- With 128 configured streams, 64 full-duplex resources must exist for media termination point application.

MTP Failover and Fallback

This section describes how MTP devices failover and fallback when the Cisco Unified CallManager to which they are registered becomes unreachable. This section also explains conditions that can affect calls that are associated with an MTP device, such as MTP reset or restart.

- Active Cisco Unified CallManager Becomes Inactive, page 27-5
- Resetting Registered MTP Devices, page 27-6

Active Cisco Unified CallManager Becomes Inactive

The following description gives the MTP device recovery methods when the MTP is registered to a Cisco Unified CallManager that goes inactive:

- If the primary Cisco Unified CallManager fails, the MTP attempts to register with the next available Cisco Unified CallManager in the Cisco Unified CallManager Group that is specified for the device pool to which the MTP belongs.
- The MTP device reregisters with the primary Cisco Unified CallManager as soon as it becomes available after a failure and is currently not in use.

- The system maintains the calls or conferences that were active in call preservation mode until all parties disconnect. The system does not make supplementary services available.
- If an MTP attempts to register with a new Cisco Unified CallManager and the register acknowledgment is never received, the MTP registers with the next Cisco Unified CallManager.

Resetting Registered MTP Devices

The MTP devices will unregister and then disconnect after a hard or soft reset. After the reset completes, the devices reregister with the Cisco Unified CallManager.

Dependency Records

To find what media resource groups a specific media termination point is using, choose Dependency Records from the drop-down list box and click **Go** from the Cisco Unified CallManager Administration Media Termination Point Configuration window. The Dependency Records Summary window displays information about media resource groups that are using the media termination point. To find out more information about the media resource group, click the media resource group, 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 and Deleting a Media Resource Group in the *Cisco Unified CallManager Administration Guide*.

Software MTP Performance Monitoring and Troubleshooting

The Real Time Monitoring Tool counters for media termination point allow you to monitor the number of media termination points that are currently in use, the number of media termination points that are currently registered with Cisco Unified CallManager but are not currently in use, and the number of times that a media termination point was requested for a call, but no resources were available. For more information about Real Time Monitoring Tool counters, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Cisco Unified CallManager writes all errors for the media termination point to the Local SysLog. In Cisco Unified CallManager Serviceability, you can set traces for the Cisco IP Voice Media Streaming Application service; to troubleshoot most issues, you must choose the Significant or Detailed option for the service, not the Error option. After you troubleshoot the issue, change the Debug Trace Level back to the Error option.

Cisco Unified CallManager generates registration and connection alarms for media termination point in Cisco Unified CallManager Serviceability. For more information on alarms, refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System Guide*.

If you need technical assistance, locate and review software MTP logs from /var/log/active/cm/trace/cms/sdi/cms*.* and /var/log/active/cm/trace/ccm before you contact your Cisco Unified Communications partner or the Cisco Technical Assistance Center (TAC).

Software MTP Configuration Checklist

Table 27-2 provides a checklist to configure MTP.

Table 27-2 MTP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Determine the number of MTP resources that are needed and the number of MTP devices that are needed to provide these resources.	Planning Your Software MTP Configuration, page 27-3
Step 2	Verify that the Cisco IP Voice Media Streaming Application service is activated and running on the server to which you are adding an MTP.	*Cisco Unified CallManager Serviceability Administration Guide* *Cisco Unified CallManager Serviceability System Guide*
Step 3	Add and configure the MTPs.	Configuring a Media Termination Point, *Cisco Unified CallManager Administration Guide*
Step 4	Add the new MTPs to the appropriate media resource groups.	Media Resource Management, page 22-1 Media Resource Group Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 5	Restart the MTP device.	Configuring a Media Termination Point, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topics

- Media Resource Management, page 22-1
- Transcoders, page 25-1
- Cisco DSP Resources for Transcoding, Conferencing, and MTP, page 28-1

Additional Cisco Documentation

- Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide*
- Media Resource Group Configuration Settings, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified Communications Solution Reference Network Design*

Cisco DSP Resources for Transcoding, Conferencing, and MTP

This chapter describes how Cisco digital signal processor (DSP) resources are used for transcoding and conferencing. The modules, which are available for use with Cisco Unified CallManager, can perform conferencing, Media Termination Point (MTP), and transcoding services in addition to serving as a PSTN gateway.

This chapter covers the following topics:

- Understanding Cisco DSP Resources, page 28-1
- Hardware-Based MTP/ Transcoding Services, page 28-2
- Hardware-Based Conferencing Services, page 28-4
- Supported Cisco Catalyst Gateways and Cisco Access Routers, page 28-5
- Where to Find More Information, page 28-10

Understanding Cisco DSP Resources

DSP resources on the Cisco gateway, for example, Catalyst 4000 (WS-X4604-GWY), Catalyst 6000 (WS-6608-T1 or WS-6608-E1), Cisco 2600, Cisco 2600XM, Cisco 2800, Cisco 3600, Cisco 3700, Cisco 3800, or Cisco VG200, provide hardware support for IP telephony features that are offered by Cisco Unified CallManager. These features include hardware-enabled voice conferencing, hardware-based MTP support for supplementary services, and transcoding services.

Note Verify with your Cisco account manager which devices support conferencing, media termination points, and transcoding services.

The DSP resource management (DSPRM) maintains the state for each DSP channel and the DSP. DSPRM maintains a resource table for each DSP. The following responsibilities belong to DSPRM:

- Discover the on-board DSP SIMM modules and, based on the user configuration, determine the type of application image that a DSP uses.
- Reset DSPs, bring up DSPs, and download application images to DSP.
- Maintain the DSP initialization states and the resource states and manage the DSP resources (allocation, deallocation, and error handling of all DSP channels for transcoding and conferencing).

- Interface with the backplane Protocol Control Information (PCI) driver for sending and receiving DSP control messages.
- Handle failure cases, such as DSP crashes and session terminations.
- Provide a keepalive mechanism between the DSPs and the primary and backup Cisco Unified CallManagers. The primary Cisco Unified CallManager can use this keepalive to determine when DSPs are no longer available.
- Perform periodic DSP resource checks.

When a request is received from the signaling layers for a session, the system assigns the first available DSP from the respective pool (transcoding or conferencing), as determined by media resource groups and media resource group lists, along with the first available channel. DSPRM maintains a set of MAX limits (such as maximum conference sessions per DSP or maximum transcoding session per DSP) for each DSP.

A switchover occurs when a higher order Cisco Unified CallManager becomes inactive or when the communication link between the DSPs and the higher order Cisco Unified CallManager disconnects. A switchback occurs when the higher order Cisco Unified CallManager becomes active again and DSPs can switch back to the higher order Cisco Unified CallManager. During a switchover and switchback, the gateway preserves active calls. When the call ends, the gateway detects RTP inactivity, DSP resources release, and updates occur on the Cisco Unified CallManager.

Hardware-Based MTP/ Transcoding Services

Introducing the WAN into an IP telephony implementation forces the issue of voice compression. After a WAN-enabled network is implemented, voice compression between sites represents the recommended design choice to save WAN bandwidth. This choice presents the question of how WAN users use the conferencing services or IP-enabled applications, which support only G.711 voice connections. Using hardware-based Media Termination Point (MTP)/transcoding services to convert the compressed voice streams into G.711 provides the solution.

The MTP service can act either like the original software MTP resource or as a transcoding MTP resource. An MTP service can provide supplementary services such as hold, transfer, and conferencing when the service is using gateways and clients that do not support the H.323v2 feature of EmptyCapabilitiesSet. The MTP, provided by the Cisco IP Voice Media Streaming Application service, can be activated as co-resident with Cisco Unified CallManager or activated separately without Cisco Unified CallManager. Both of these services operate on the Cisco Unified CallManager appliance (server). The Cisco IP Voice Media Streaming Application service installs as a component with Cisco Unified CallManager; however, for a dedicated MTP server, the Cisco CallManager service would not be activated (only the Cisco Voice IP Voice Media Streaming Application service).

When MTP is running in software on Cisco Unified CallManager, the resource supports 48 MTP sessions. When MTP is running on a separate Cisco Unified CallManager appliance (server), the resource supports up to 128 MTP sessions. In addition, Cisco Voice Gateway Routers also have the ability to provide MTP services.

Observe the following design capabilities and requirements for MTP transcoding:

- Provision MTP transcoding resources appropriately for the number of IP WAN callers to G.711 endpoints.
- Each transcoder has its own jitter buffer of 20-40 ms.

The following summary gives caveats that apply to MTP transcoding:

- Make sure that each Cisco Unified CallManager has its own configured MTP transcoding resource.
- If transcoding is required between Cisco Unified CallManager clusters, make sure that the intercluster trunk is configured with an MTP resource. All calls between Cisco Unified CallManager clusters will go through the MTPs.
- If all *n* MTP transcoding sessions are utilized, and an *n* + 1 connection is attempted, the next call will complete without using the MTP transcoding resource. If this call attempted to use the software MTP function to provide supplementary services, the call would connect, but any attempt to use supplementary services would fail and could result in call disconnection. If the call attempted to use the transcoding features, the call would connect directly, but no audio would be received. If a transcoder is required but not available, the call would not connect.

For specific information on the number of sessions that are supported, see the "Supported Cisco Catalyst Gateways and Cisco Access Routers" section on page 28-5.

IP-to-IP Packet Transcoding and Voice Compression

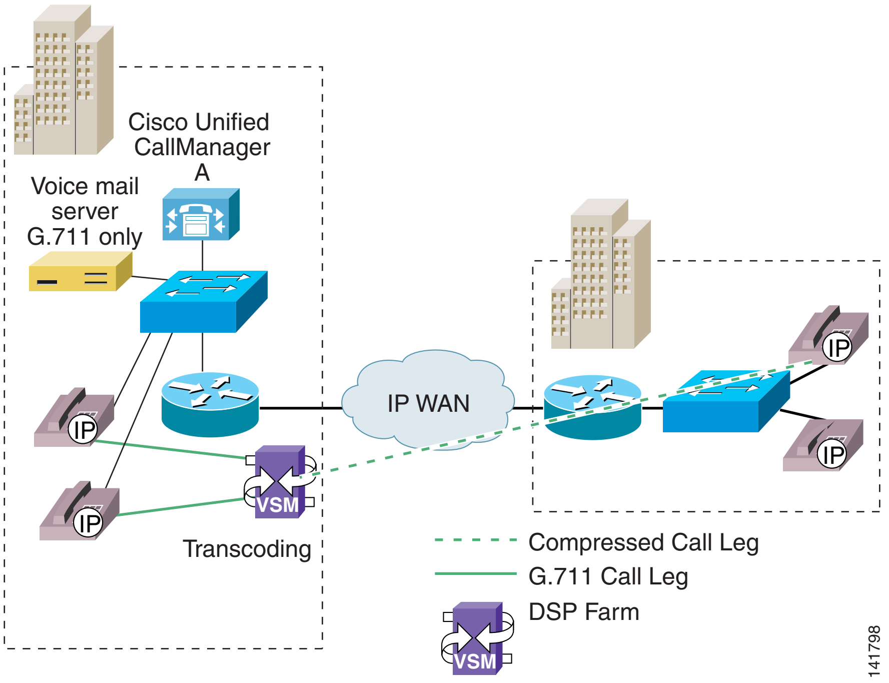
You can configure voice compression between IP phones through the use of regions and locations in Cisco Unified CallManager. However, the Cisco Catalyst conferencing services and some applications currently support only G.711, or uncompressed, connections. For these situations, MTP transcoding or packet-to-packet gateway functionality provides modules for the Cisco Catalyst 4000 and Cisco Catalyst 6000. A packet-to-packet gateway designates a device with DSPs that has the job of transcoding between voice streams by using different compression algorithms. For example, a user on an IP phone at a remote location calls a user at the central location. Cisco Unified CallManager instructs the remote IP phone to use compressed voice, or G.729a, only for the WAN call. If the called party at the central site is unavailable, the call may roll to an application that supports G.711 only. In this case, a packet-to-packet gateway transcodes the G.729a voice stream to G.711 to leave a message with the voice-messaging server.

Voice Compression, IP-to-IP Packet Transcoding, and Conferencing

Connecting sites across an IP WAN for conference calls presents a complex scenario. In this scenario, the modules must perform the conferencing service as well as the IP-to-IP transcoding service to uncompress the WAN IP voice connection. In Figure 28-1, a remote user joins a conference call at the central location. This three-participant conference call uses seven DSP channels on the Catalyst 4000 module and three DSP channels on the Cisco Catalyst 6000. The following list gives the channel usage:

- Cisco Catalyst 4000
  - One DSP channel to convert the IP WAN G.729a voice call into G.711
  - Three conferencing DSP channels to convert the G.711 streams into TDM for the summing DSP
  - Three channels from the summing DSP to mix the three callers together
- Cisco Catalyst 6000
  - Three conferencing DSP channels. On the Cisco Catalyst 6000, all voice streams get sent to single logical conferencing port where all transcoding and summing takes place.

Figure 28-1 Multisite WAN Using Centralized MTP Transcoding and Conferencing Services



IP-to-IP Packet Transcoding Across Intercluster Trunks

Intercluster trunks connect Cisco Unified CallManager clusters. Intercluster trunks allocate a transcoder on a dynamic basis.

The Cisco Catalyst 6000 module uses the MTP service regardless of whether transcoding is needed for a particular intercluster call. Cisco Unified CallManager supports compressed voice call connection through the MTP service if a hardware MTP is used.

The following list gives intercluster MTP/transcoding details:

- Outbound intercluster calls will use an MTP/transcoding resource from the Cisco Unified CallManager from which the call originates.
- Inbound intercluster call will use the MTP/resource from the Cisco Unified CallManager that terminates the inbound intercluster trunk.
- Allocate additional DSP MTP/transcoding resources to Cisco Unified CallManagers terminating intercluster trunks.
- For compressed callers, you can accurately provision the MTP transcoding resources.

Hardware-Based Conferencing Services

Hardware-enabled conferencing designates the ability to support voice conferences by using DSPs to perform the mixing of voice streams to create multiparty conference sessions. The voice streams connect to conferences through packet or time-division-multiplexing (TDM) interfaces.

The network modules, depending on the type, support both uncompressed and compressed VOIP conference calls. The modules use Skinny Client Control Protocol to communicate with Cisco Unified CallManager to provide conferencing services. When the conferencing service registers with Cisco Unified CallManager, it announces that only G.711 calls can connect to the conference. If any compressed calls request to join a conference, Cisco Unified CallManager connects them to a transcoding port first to convert the compressed call to G.711.

Observe the following recommendations when you are configuring conferencing services:

- When you are provisioning an enterprise with conference ports, first determine how many callers will attempt to join the conference calls from a compressed Cisco Unified CallManager region. After you know the number of compressed callers, you can accurately provision the MTP transcoding resources.
- Conference bridges can register with more than one Cisco Unified CallManager at a time, and Cisco Unified CallManagers can share DSP resources through the Media Resource Manager (MRM).

For specific information on the number of sessions that are supported, see the "Supported Cisco Catalyst Gateways and Cisco Access Routers" section on page 28-5.

Supported Cisco Catalyst Gateways and Cisco Access Routers

For specific information on the number of supported conferencing, transcoding, and MTP sessions for Cisco Catalyst Gateways and Cisco Access Routers, see the following sections:

- Cisco Catalyst 4000 WS-X4604-GWY, page 28-5
- Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1, page 28-6
- Cisco 2600, Cisco 2600XM, Cisco 2800, Cisco 3600, Cisco 3700, Cisco 3800, and Cisco VG200 for NM-HDV, page 28-8
- Cisco 2600XM, Cisco 2691, Cisco 2800, Cisco 3600, Cisco 3700, and Cisco 3800 for NM-HD and NM-HDV2, page 28-8

Cisco Catalyst 4000 WS-X4604-GWY

The PSTN gateway and voice services module for the Cisco Catalyst 4003 and 4006 switches supports three analog voice interface cards (VICs) with two ports each or one T1/E1 card with two ports and two analog VICs. Provisioning choices for the VIC interfaces include any combination of Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), or Ear & Mouth (E&M). Additionally, when configured as an IP telephony gateway from the command-line interface (CLI), this module can support conferencing and transcoding services.

You can configure the Cisco Catalyst 4000 voice gateway module in either toll bypass mode or gateway mode; however, you can configure the module conferencing and transcoding resources only in gateway mode. Gateway mode designates the default configuration. From the CLI, you can change the conferencing-to-transcoding ratios. After the gateway mode is enabled, the 24 DSPs (4 SIMMs with 6 DSPs each) for the module occur as described in the following bullets:

- Over the PSTN gateway using G.711 only—96 calls
- In a G.711 conference only—24 conference participants; maximum of 4 conferences of 6 participants each

  Unlike the WS-X6608-x1, which can mix all conference call participants, the Cisco Catalyst 4000 WS-X4604-GWY module sums only the three dominant speakers. The WS-X4604-GWY dynamically adjusts for the dominant speakers and determines dominance primarily by voice volume, not including any background noise.

Caution The Cisco Catalyst 4000 conferencing services support G.711 connections only, unless an MTP transcoding service is used.

- Transcoding to G.711—16 MTP transcoding sessions

The following information applies to the Cisco Catalyst 4000 module:

- The WS-X4604-GWY uses a Cisco IOS interface for initial device configuration. All additional configuration for voice features takes place in Cisco Unified CallManager.
- The WS-X4604-GWY can operate as a PSTN gateway (toll bypass mode) as well as a hardware-based transcoder or conference bridge (gateway mode). To configure this module as a DSP farm (gateway mode), enter one or both of the following CLI commands:

```
voicecard conference
voicecard transcode
```

- The WS-X4604-GWY requires its own local IP address in addition to the IP address for Cisco Unified CallManager. Specify a loopback IP address for the local Signaling Connection Control Part.
- You can define a primary, secondary, and tertiary Cisco Unified CallManager for both the conferencing and MTP transcoding services.

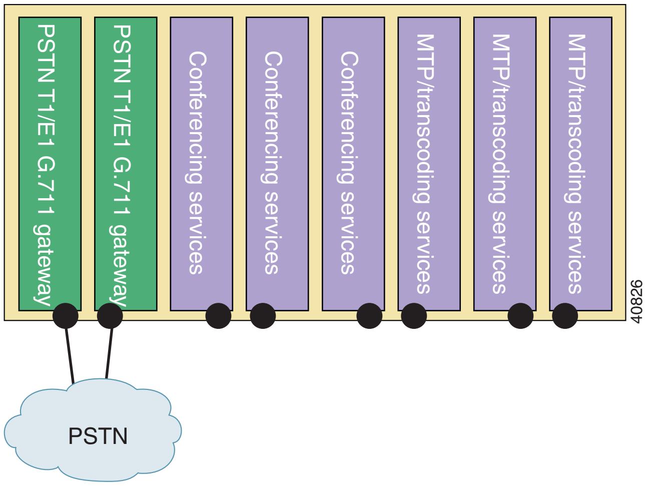
Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1

The WS-6608-T1 (or WS-6608-E1 for European countries) designates the same module that provides T1 or E1 PSTN gateway support for the Cisco Catalyst 6000. This module comprises eight channel-associated-signaling (CAS) or primary rate interface (PRI) interfaces, each of which has its own CPU and DSPs. After the card is added from Cisco Unified CallManager as a voice gateway, you configure it as a conferencing or MTP transcoding resource. Each port acts independently of the other ports on the module. Specifically, you can configure each port only as a PSTN gateway interface, a conferencing node, or an MTP transcoding node. In most configurations, configure a transcoding resource for each conferencing resource.

Whether acting as a PSTN gateway, a conferencing resource, or an MTP transcoding resource, each port on the module requires its own IP address. Configure the port to have either a static IP address or an IP address that the DHCP provides. If a static IP is entered, you must also add a TFTP server address because the ports actually get all configuration information from the downloaded TFTP configuration file.

Figure 28-2 shows one possible configuration of the Cisco Catalyst 6000 voice gateway module. This diagram shows two of the eight ports of the module as configured in PSTN gateway mode, three ports in conferencing mode, and three ports in MTP transcoding mode.

Figure 28-2 Cisco Catalyst 6000 Voice Gateway Module



After a port is configured through the Cisco Unified CallManager interface, each port can support one of the following configurations:

- WS-6608-T1 over the PSTN gateway —24 calls per physical DS1 port; 192 calls per module
- WS-6608-E1 over the PSTN gateway—30 calls per physical DS1 port; 240 calls per module
- For a G.711 or G.723 conference—32 conferencing participants per physical port; maximum conference size of 16 participants
- For a G.729 conference—24 conferencing participants per physical port; maximum conference size of 16 participants

Tip After the WS-X6608 is added as a T1 or E1 Cisco gateway, you can configure it, on a per-port basis, for conferencing services.

On the Cisco Catalyst 6000, conferencing services cannot cross port boundaries.

The following capacities apply to simultaneous transcoding and conferencing:

- For transcoding from G.723 to G.711—32 MTP transcoding sessions per physical port; 256 sessions per module
- For transcoding from G.729 to G.711—24 MTP transcoding sessions per physical port; 192 sessions per module

Cisco 2600, Cisco 2600XM, Cisco 2800, Cisco 3600, Cisco 3700, Cisco 3800, and Cisco VG200 for NM-HDV

NM-HDV supports the previous Cisco gateways.

The following list represents the maximum number of sessions:

- G.711, G.729, GSM FR, and GSM EFR conference sessions—Per network module, 15

Tip Maximum participants per conference session equals 6.

- Transcoding from G.711 to G.729—Per network module, 60
- Transcoding from G.711 to GSM FR/GSM EFR—Per network module, 45

Caution On these gateways, transcoding services cannot cross port boundaries.

Cisco MTP transcoding service only supports HBR codec to G.711 conversion and vice versa. No support exists for LBR-to-LBR codec conversion.

Cisco 2600XM, Cisco 2691, Cisco 2800, Cisco 3600, Cisco 3700, and Cisco 3800 for NM-HD and NM-HDV2

Tip The NM-HDV2 does not support the Cisco 3660.

The following list represents the maximum number of sessions that are available for conferences, transcoding, and MTP for HM-HD and NM-HDV2:

Per NM-HD-1V/2V

- G.711 only conference—8 sessions
- G.729, G.729a, G.729ab, and G.729b conference—2 sessions
- GSM FR conference—Not applicable
- GSM EFR conference—Not applicable

Tip Maximum number of participants per conference equals 8.

- Transcoding for G.711 to G.729a/G.729ab/GSMFR—8 sessions
- Transcoding for G.711 to G.729/G.729b/GSM EFR—6 sessions

Per NM-HDV2

- G.711 only conference—50 sessions
- G.729, G.729a, G.729ab, G.729b conference—32 sessions
- GSM FR conference—14 sessions

- GSM EFR conference—10 sessions
- Transcoding for G.711 to G.729a/G.729ab/GSMFR—128 sessions
- Transcoding for G.711 to G.729/G.729b/GSM EFR—96 sessions

Tip For a software MTP (DSP-less with same packetization period for both devices supporting G.711 to G.711 or G.729 to G.729 codecs), 500 sessions can occur per gateway; for a hardware MTP (with DSP, using G.711 codec only), 200 sessions can occur per NM-HDV2 and 48 per NM-HD.

Per 2801/2811 (2 PVDM2-64)

- G.711 only conference—50 sessions
- G.729, G.729a, G.729ab, G.729b conference—16 sessions
- GSM FR conference—7 sessions
- GSM EFR conference—5 sessions
- Transcoding for G.711 to G.729a/G.729ab/GSMFR—64 sessions
- Transcoding for G.711 to G.729/G.729b/GSM EFR—48 sessions

Per 2821/2851 (3 PVDM2-64)

- G.711 only conference—50 sessions
- G.729, G.729a, G.729ab, G.729b conference—24 sessions
- GSM FR conference—10 sessions
- GSM EFR conference—8 sessions
- Transcoding for G.711 to G.729a/G.729ab/GSMFR—96 sessions
- Transcoding for G.711 to G.729/G.729b/GSM EFR—72 sessions

Per 3825/3845 (4 PVDM2-64)

- G.711 only conference—50 sessions
- G.729, G.729a, G.729ab, G.729b conference—32 sessions
- GSM FR conference—14 sessions
- GSM EFR conference—10 sessions
- Transcoding for G.711 to G.729a/G.729ab/GSMFR—128 sessions
- Transcoding for G.711 to G.729/G.729b/GSM EFR—96 sessions

Tip Maximum number of participants per conference equals 8.

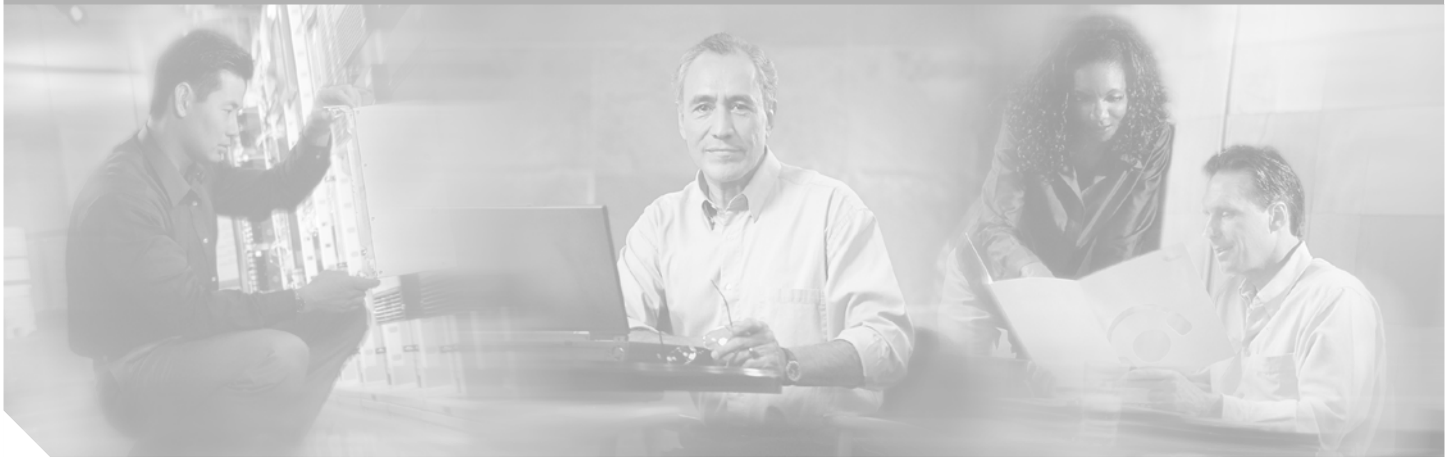
Where to Find More Information

Related Topics

- Transcoders, page 25-1
- Conference Bridges, page 24-1
- Media Termination Points, page 27-1

Additional Cisco Documentation

- *Cisco Unified CallManager Administration Guide*



PART 6

Voice Mail and Messaging Integration

CHAPTER 29

Voice Mail Connectivity to Cisco Unified CallManager

A voice-messaging system, which is an integral part of an enterprise telecommunications system, provides voice-messaging features for all users. After receiving voice messages in their mailboxes, users receive message-waiting lights on their phones. Users can retrieve, listen to, reply to, forward, and delete their messages by accessing the voice-messaging system with an internal or external call.

Note You must enter all users and their directory numbers in Cisco Unified CallManager Administration to make it possible for them to retrieve messages from a Cisco Unity voice-mail device.

Cisco Unified CallManager supports an increasing variety of voice-messaging systems and provides configuration of message-waiting indicators for all users, including those with shared line appearances.

As the size or number of Cisco Unified CallManager clusters increases in an enterprise, the likelihood that an administrator needs to deploy multiple voice-messaging systems also increases.

This chapter provides the following topics about configuring voice-messaging systems and features:

- Voice-Mail Interfaces, page 29-1
- Voice-Mail System Access, page 29-2
- Message Waiting, page 29-4
- Call Forwarding in a Multiple Voice-Mail System Environment, page 29-5
- Call Transfer with Voice-Mail Systems, page 29-6
- Where to Find More Information, page 29-7

Voice-Mail Interfaces

Cisco Unified CallManager supports both directly connected and gateway-based messaging systems. Directly connected voice-messaging systems communicate directly with Cisco Unified CallManager by using a packet protocol. A gateway-based voice-messaging system connects to Cisco Unified CallManager through analog or digital trunks that connect to Cisco gateways.

Cisco Unified CallManager interacts with voice-messaging systems by using the following types of interfaces:

- Skinny Protocol—Directly connected voice-messaging systems that use Skinny protocol could use other protocols to communicate with Cisco Unified CallManager. In Cisco Unified CallManager Administration, you configure the interface to directly connected voice-messaging systems by creating voice-mail ports. To handle multiple, simultaneous calls to a voice-messaging system, you create multiple voice-mail ports and place the ports in a line group and the line group in a route/hunt list. Directly connected voice-messaging systems send message-waiting indications by calling a message-waiting on and off number that is configured in Cisco Unified CallManager Administration. Refer to "Cisco Voice-Mail Port Configuration" in the *Cisco Unified CallManager Administration Guide*.

  When you configure security for voice-mail ports and Cisco Unity SCCP devices, a TLS connection (handshake) opens for authenticated devices after each device accepts the certificate of the other device; likewise, the system sends SRTP streams between devices; that is, if you configure the devices for encryption.

  When the device security mode equals authenticated or encrypted, the Cisco Unity TSP connects to Cisco Unified CallManager through the Cisco Unified CallManager TLS port. When the security mode equals nonsecure, the Cisco Unity TSP connects to Cisco Unified CallManager through the Cisco Unified CallManager SCCP port.

- PSTN Gateway Interfaces—H.323-based voice-messaging systems and legacy voice-messaging systems use PSTN gateway interfaces. These systems usually (but not necessarily) send message-waiting indications by using Simplified Message Desk Interface (SMDI) over an EIA/TIA-232 interface. Cisco Unified CallManager also sends call history messages to the voice messaging system using this same SMDI interface. The Cisco Messaging Interface service relays these indications to Cisco Unified CallManager. In Cisco Unified CallManager Administration, you can provision the interface to gateway-based voice-messaging systems simply by provisioning an analog FXS gateway or a digital T1/E1 gateway with CAS or PRI protocols. By creating a route group that contains individual gateway ports or T1 spans, you can enable simultaneous calls to a voice-messaging system. In addition, if the voice-messaging system uses SMDI, you must configure and run the Cisco Messaging Interface service. Refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.
- Intercluster Interfaces—A Cisco Unified CallManager in one cluster can provide access to a voice-messaging system in another cluster, if the administrator provisions the voice-mail pilot number on the intercluster trunk. Voice-messaging systems can leave messages and set message-waiting indicators for devices in other clusters if the clusters are connected by QSIG trunks.

Voice-Mail System Access

For directly connected voice-messaging systems, Cisco Unified CallManager uses directory numbers that are assigned to voice-mail ports. Administrators assign the voice-mail ports to a line group and place the line group in a route/hunt list. If multiple users attempt to access a voice-messaging system at the same time, all users have an available port for access to the voice-messaging system. When users access their voice messages, they dial the voice-mail pilot number or press the messages button on the phone.

For gateway-based voice-messaging systems, Cisco Unified CallManager uses route lists. When a user calls the route list number, the route list offers incoming calls to each port of the voice-messaging system by using a search algorithm. For gateway-based voice-messaging systems, the voice-mail pilot number specifies the route list itself.

Calls to directory numbers that are associated with voice-messaging systems cause the called voice-messaging systems to handle the call. When calls are made directly to voice-messaging systems, the system prompts the user for mailbox and password information for message retrieval.

Users can reach a voice-messaging system either by entering the voice-mail pilot number, if known, or by pressing the messages button on a Cisco 7900 series IP Phone. When a user presses the messages button, a call goes to the voice-mail pilot number that the administrator has configured for the line that is currently in use on the Cisco IP Phone. When the active line has no voice-mail pilot number configured, Cisco Unified CallManager directs voice-messaging calls to a default profile.

Voice-Mail Pilot Numbers

The voice-mail pilot number specifies the directory number that you dial to access your voice messages. Cisco Unified CallManager automatically dials the voice-messaging number when you press the messages button on your phone. Each voice-mail pilot number can belong to a different voice-messaging system.

The Voice Mail Pilot Configuration window of Cisco Unified CallManager Administration defines the voice-messaging number.

A default voice-mail pilot number exists in Cisco Unified CallManager. You can create a new default voice-mail pilot number that replaces the current default setting. Refer to the "Cisco Voice-Mail Pilot Configuration" in the *Cisco Unified CallManager Administration Guide*.

Voice-Mail Profiles

Different lines on a device can have different voice-mail profiles. For example, an administrative assistant phone can have a second line for the manager, which routes to the manager's voice-messaging system. The administrative assistant line routes to its own voice-messaging system.

Voice-mail profiles allow you to define any line-related, voice-mail information that is associated to a directory number, not a device. The voice-mail profile contains the following information:

- Voice Mail Profile Name
- Description
- Voice Mail Pilot Number
- Voice Mail Box Mask
- Default (checked if this particular profile is the default profile)

A predefined, default voice-mail profile automatically gets assigned to lines when the administrator adds a line. When you search for voice-mail profiles, "default" appears beside the profile name within the list.

A voice-mail profile takes precedence over other settings when calls are routed to a voice-messaging system. Refer to "Voice-Mail Profile Configuration" in the *Cisco Unified CallManager Administration Guide*.

Message Waiting

For directly connected voice-messaging systems, you can configure message waiting by using a single configuration window in Cisco Unified CallManager Administration. The Message Waiting Configuration window defines directory numbers for message-waiting on and message-waiting off indicator. A directly connected voice-messaging system uses the specified directory number to set or to clear a message-waiting indication for a particular Cisco Unified IP Phone.

The Message Waiting Configuration window of Cisco Unified CallManager Administration provides for the following information:

- Confirmation of multiple message-waiting on and off numbers for a Cisco Unified CallManager cluster
- Explicit association of a message-waiting search space with each message-waiting on and off number
- Validation of the message-waiting number and calling search space entry
- Search for conflicting numbers in the numbering plan.

Message Waiting Indication

When a caller leaves a message in a mailbox, the voice-messaging system sends a message-waiting indication on to the party that received the voice message. Similarly, when the owner of a voice mailbox deletes all pending voice messages, the voice-messaging system sends a messaging-waiting indication off to inform the voice-mailbox owner that no more messages are pending.

Cisco Unified CallManager enables administrators to configure how to turn on the handset indicator of Cisco Unified IP Phones 7940 and 7960 for pending voice messages. You can configure Cisco Unified CallManager to do one of the following actions:

- Light the message-waiting lamp and display the prompt if a message is waiting on primary line.
- Display the prompt if a message is waiting on primary line.
- Light the message-waiting lamp if a message is waiting on primary line.
- Light the message-waiting lamp and display the prompt if a message is waiting on any line.
- Display only the prompt, if a message is waiting on any line.
- Display only the message-waiting lamp, if a message is waiting on any line
- Do not light the message-waiting lamp or display the prompt

You can set the message-waiting indication policy by using two different methods:

- Directory Number Configuration—Use the Message Waiting Lamp Policy field to set when the handset lamp turns on for a given line. Use the following available settings:
  - Use System Policy
  - Light and Prompt
  - Prompt Only
  - Light Only
  - None

- Service Parameter Configuration (for the Cisco CallManager service)—Use the Message Waiting Lamp Policy clusterwide service parameter to set the message-waiting indication policy for all Cisco 7900 series IP Phones. Use the following available settings:
  - Primary Line - Light and Prompt
  - Primary Line - Prompt Only
  - Primary Line - Light Only
  - Light and Prompt
  - Prompt Only
  - Light Only
  - None

The message-waiting policy that you choose depends on the needs of your users. For example, an administrative assistant, who shares the manager's directory number as a secondary directory number, may want to have the policy set to Light and Prompt. The administrator can see whether the manager's line has pending voice messages. General office members, who share a line appearance with a coworker, might set the policy, so the indicator lights only when messages are pending for the primary line appearance.

For customers who do not have complex message-waiting indicator requirements, you can use the Cisco CallManager service parameter to dictate the conditions under which Cisco Unified CallManager turns on the message-waiting lamp.

Note Users can set the message-waiting indication policy on their phones by using the Cisco Unified CallManager User Options window. For more information, refer to the user guide for the Cisco Unified IP Phone.

Call Forwarding in a Multiple Voice-Mail System Environment

Voice-messaging systems support a maximum number of users just as Cisco Unified CallManager supports a maximum number of users.

To ensure that calls are forwarded to the voice-messaging system that is associated with the user for whom a voice message is intended, the Call Forward feature gets modified when calls are forwarded to voice-messaging systems.

Cisco Unified CallManager supports multiple voice-mail pilot numbers (profiles). Each pilot number can belong to a different voice-messaging system. Configure the voice-mail pilot profile on a line-by-line basis. Cisco Unified CallManager forwards a voice-mail call to the voice-messaging system of the original redirect endpoint (directory number) if it has the voice-mail pilot profile.

One limitation exists for intercluster call forwarding. When a call is forwarded from another cluster and then sent to voice mail, Cisco Unified CallManager forwards the call to the voice-messaging system of the first redirect endpoint in the cluster. This occurs because Cisco Unified CallManager does not have the voice-mail pilot profile of the original endpoint in the other cluster. However, if a QSIG trunk links the clusters, the forwarded call will have the correct voice mailbox number but not the voice mail pilot number.

The Directory Number Configuration window of Cisco Unified CallManager Administration contains Call Forward and Pickup Settings. If the Voice Mail check box is chosen, Cisco Unified CallManager can Forward All, Forward Busy, or Forward No Answer to all devices for the chosen voice mail profile.

Examples

Intracluster call-forwarding chains where the final forwarding phone has used the Forward To Voice Mail option

A call forwards-all from a phone that is served by one voice-mail pilot to a phone that is served by another voice-mail pilot. The second phone forwards to voice mail. Cisco Unified CallManager delivers the call to the voice-mail pilot number that is associated with the first phone.

Intracluster call-forwarding chains where the final forwarding phone has not used the Forward To Voice Mail option

A call forwards-all from a phone that is served by one voice-mail pilot to a phone that is served by another voice-mail pilot. The second phone forwards to voice mail, but the voice-mail pilot number was entered as a specific numerical destination and not as a forward-to voice mail.
Cisco Unified CallManager delivers the call to the voice-mail pilot number that is associated with the last phone.

Intracluster call-forwarding chains with CTI

When Cisco Unified CallManager Attendant Console or other CTI applications take control of a call, they often choose to eliminate information about the original call, so the next destination receives voice messages. Cisco Unified CallManager must direct the call to the voice-messaging system that manages the voice mailbox that Cisco Unified CallManager reports as the target voice mailbox, as shown in the following examples.

A call arrives at a phone, which forwards to the attendant console, the calling user dials-by-name, and Cisco Unified CallManager extends the call to a destination. The destination forwards to voice mail. Cisco Unified CallManager delivers the call to the voice-messaging number that is associated with the destination that the calling user chose, not the attendant console.

In another example, phone A forwards all calls to phone B. A call arrives at the attendant console, and the attendant console sends the call to phone A. Cisco Unified CallManager forwards the call to phone B. If no one answers the call, Cisco Unified CallManager forwards the call to voice mail. Because the call was originally for phone A, the message goes to the voice mailbox of phone A, not phone B.

Intercluster call-forwarding chains

In an intercluster call scenario, phone A on a Cisco Unified CallManager calls phone B on the same Cisco Unified CallManager. The call forwards over an intercluster trunk to Cisco Unified CallManager, which extends the call to phone C. Phone C forwards to voice mail. Cisco Unified CallManager extends the call to the voice-messaging system that is associated with phone C, but reports the extension number of phone B.

No available voice-mail pilot number information exists about phone B because of the intercluster boundary. Therefore, Cisco Unified CallManager sends the call to the voice-mail pilot number that is associated with the final destination but reports the directory number that was passed from the PBX to Cisco Unified CallManager as the voice mailbox.

Call Transfer with Voice-Mail Systems

Users, who have reached a voice-messaging system over a Cisco analog FXS gateway or a Cisco 6608 T1 CAS gateway, can transfer out of the voice-messaging system to another destination. By responding to a voice-messaging prompt, the user enters a number. The voice-messaging system initiates the action by using a hookflash transfer. Cisco Unified CallManager responds by doing a blind transfer of the call to the target number. When the call transfer completes, the voice channel that connected the original call to the voice-messaging system gets released.

Configure hookflash detection timers for the Cisco Catalyst 6000 T1 Gateway by using Cisco Unified CallManager Administration Gateway Configuration (see Adding a Non-IOS MGCP Gateway in the *Cisco Unified CallManager Administration Guide*).

Note Only E&M T1 ports support the hookflash transfer.

Where to Find More Information

Additional Cisco Documentation

- Cisco Voice-Mail Port Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Voice Mail Port Wizard, *Cisco Unified CallManager Administration Guide*
- Message Waiting Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Voice-Mail Pilot Configuration, *Cisco Unified CallManager Administration Guide*
- Voice-Mail Profile Configuration, *Cisco Unified CallManager Administration Guide*
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*

SMDI Voice Mail Integration

Simplified Message Desk Interface (SMDI) defines a way for a phone system to provide voice-messaging systems with the information that the system needs to intelligently process incoming calls. Each time that the phone system routes a call, it sends an SMDI message through an EIA/TIA-232 connection to the voice-messaging system that tells it the line that it is using, the type of call that it is forwarding, and information about the source and destination of the call.

The SMDI-compliant voice-messaging system connects to Cisco Unified CallManager in two ways:

- Using a standard serial connection to the Cisco Unified CallManager
- Using POTS line connections to a Cisco analog FXS gateway

This section covers the following topics:

- SMDI Voice Mail Integration Requirements, page 30-1
- Port Configuration for SMDI, page 30-2
- Cisco Messaging Interface Redundancy, page 30-2
- SMDI Configuration Checklist, page 30-4
- Where to Find More Information, page 30-5

SMDI Voice Mail Integration Requirements

The Cisco Messaging Interface service allows you to use an external voice-messaging system with Cisco CallManager Release 3.0 and later.

The voice-messaging system must meet the following requirements:

- The voice-messaging system must have a simplified message desk interface (SMDI) that is accessible with a null-modem EIA/TIA-232 cable (and an available serial port).
- The voice-messaging system must use analog ports for connecting voice lines.
- The Cisco Unified CallManager server must have an available serial or USB port for the SMDI connection.
- A Cisco Access Analog Station Gateway, Cisco Catalyst 6000 24-port FXS gateway, Cisco VG200 gateway, or Cisco Catalyst 6000 8-port T1 gateway that is configured with FXS ports must be installed and configured.
- You must ensure that gateways are configured in a route pattern. Refer to the "Route Pattern Configuration" chapter in the *Cisco Unified CallManager Administration Guide* for more information.

Port Configuration for SMDI

Previous releases of Cisco Unified CallManager required a specific configuration for voice-messaging integration using the SMDI and the Cisco Messaging Interface. This older configuration method for FXS ports required each individual port of an analog access gateway (Cisco AS-2, Cisco AS-4, Cisco AS-8, or Cisco Catalyst 6000 24 Port FXS gateway) to be explicitly configured as a separate entry in a route group. The relative position within the route list/route group of each analog access port determined the SMDI port number that the Cisco Messaging Interface reported.

For Cisco CallManager Release 3.0(5) and later releases, you can configure the SMDI port number through Cisco Unified CallManager Administration.

If you use the Cisco Catalyst 6000 8-port T1 gateway (6608) to interface with voice-messaging system, you must configure the SMDI base port for each T1 span.

To use the new SMDIPortNumber configuration, perform the following steps:

1. Modify each analog access port that connects to the voice-messaging system and set the SMDIPortNumber equal to the actual port number on the voice-messaging system to which the analog access port connects.

   With this first step, you do not need to change any route lists/route groups. The newly configured SMDIPortNumber(s) override any existing route list/route group configuration that was set up for the devices that connect to the voice-messaging system.

2. To take advantage of reduced Cisco Unified CallManager signaling requirements with this new configuration, change each analog access device that is in a route group that was set up for the older method of configuration from multiple entries that identify individual ports on the device to a single entry in the route group that identifies "All Ports" as the port selection.

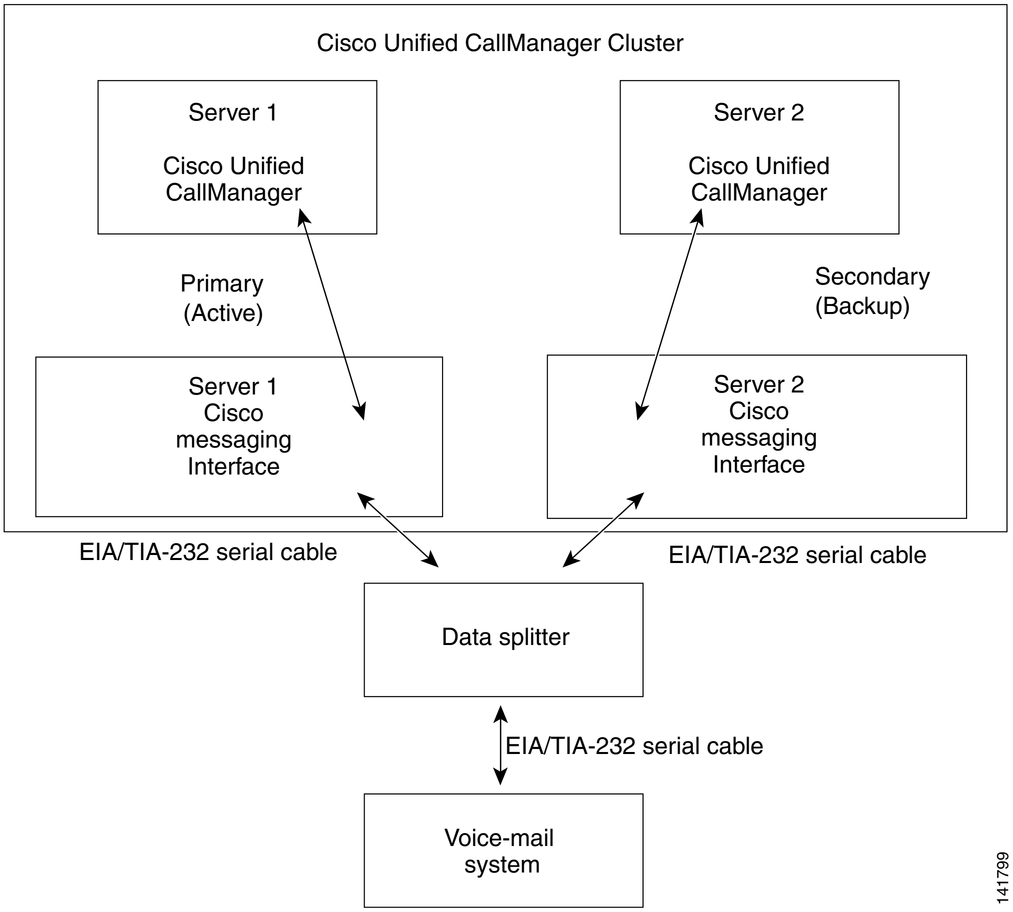
The selection order of each of these device entries differs or does not differ.

Cisco Messaging Interface Redundancy

Most voice-messaging systems that rely on an EIA/TIA-232 serial cable (previously known as a RS-232 cable) to communicate with phone systems only have one serial port. You can achieve Cisco Messaging Interface redundancy by running two or more copies of the Cisco Messaging Interface service on different servers in a Cisco Unified CallManager cluster and using additional hardware including a data splitter that is described later in this section.

Each copy of Cisco Messaging Interface connects to a primary and backup Cisco Unified CallManager and registers to the Cisco Unified CallManager by using the same VoiceMailDn and VoiceMailPartition service parameter values. The Cisco Messaging Interface with the higher service priority (the active Cisco Messaging Interface service) handles the SMDI responsibilities. If this Cisco Messaging Interface encounters problems, another one can take over. Figure 30-1 illustrates one of many layouts that provide Cisco Messaging Interface redundancy.

Figure 30-1 Cisco Messaging Interface Redundancy



Note To achieve Cisco Messaging Interface redundancy, you must have a device such as the data splitter as shown in Figure 30-1 to isolate the SMDI messaging from the various Cisco Messaging Interface services. You cannot use an ordinary Y-shaped serial cable to combine the EIA/TIA-232 streams together.

The data splitter that you connect to your voice-messaging system, such as the B&B Electronics modem data splitter (models 232MDS and 9PMDS), must have the following characteristics:

- High reliability
- Bidirectional communication
- Minimal transmission delay
- No external software support (desired)
- No extra EIA/TIA-232 control line operations (desired)

The 232MDS includes two DB25 male ports and one DB25 female port. The 9PMDS represents a DB9 version of this modem data splitter. These switches enable Cisco Messaging Interface redundancy with the following limitations when you set the ValidateDNs Cisco Messaging Interface service parameter to *Off*:

- Two Cisco Messaging Interfaces cannot transmit SMDI messages simultaneously. Under extreme circumstances, you may experience network failures that break your Cisco Unified CallManager cluster into two unconnected pieces. In the unlikely event that this occurs, both copies of Cisco Messaging Interface may become active, which leads to the possibility that they may simultaneously transmit SMDI messages to the voice-messaging system. If this happens, the collision could result in an erroneous message to the voice-messaging system, which may cause a call to be mishandled.

SMDI Configuration Checklist

Table 30-1 provides an overview of the steps that are required to integrate voice-messaging systems that are using SMDI.

Table 30-1 SMDI Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Add and configure gateway ports. If you are configuring an Octel system and you are using a Cisco Catalyst 6000 24 Port FXS Analog Interface Module or AST ports, make sure to set the Call Restart Timer field on each port to 1234.	Adding Gateways to Cisco Unified CallManager, *Cisco Unified CallManager Administration Guide*
Step 2	Create a route group and add the gateway ports that you configured in Step 1 to the route group.	Configuring a Route Group, *Cisco Unified CallManager Administration Guide*
Step 3	Create a route list that contains the route group that was configured in Step 2.	Adding a Route List, *Cisco Unified CallManager Administration Guide*
Step 4	Create a route pattern.	Configuring a Route Pattern, *Cisco Unified CallManager Administration Guide*
Step 5	Activate, configure, and run the Cisco Messaging Interface service.	*Cisco Unified CallManager Serviceability Administration Guide* Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
Step 6	Configure Cisco Messaging Interface trace parameters.	*Cisco Unified CallManager Serviceability Administration Guide* *Cisco Unified CallManager Serviceability System Guide*
Step 7	Configure your voice-messaging system and connect the voice-messaging system to Cisco Unified CallManager with an EIA/TIA-232 cable.	Refer to the documentation provided with your system.

Where to Find More Information

Additional Cisco Documentation

- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified Communications Solution Reference Network Design (SRND)*

CHAPTER 31

Cisco Unity Messaging Integration

Cisco Unity comprises a communications solution that delivers voice messaging and unified messaging in a unified environment.

Unified messaging means that users can manage all message types from the same Inbox. Cisco Unity works in concert with an Exchange server or (for Cisco Unity 4.0 and later) a Domino server to collect and store all messages—both voice and e-mail—in one message facility. Users can then access voice and e-mail messages on a computer, through a touchtone phone, or over the Internet.

For complete, step-by-step instructions on how to integrate Cisco Unified CallManager with the Cisco Unity messaging system, refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity.*

Note For information on how to integrate Cisco Unified CallManager with the Cisco Unity Connection messaging system, refer to the *Cisco Unified CallManager 5.0 SCCP Integration Guide for Cisco Unity Connection 1.1* or the *Cisco Unified CallManager 5.0 SIP Trunk Integration Guide for Cisco Unity Connection 1.1*.

This section covers the following topics:

- System Requirements, page 31-1
- Integration Description, page 31-2
- Cisco Unity Cisco Unified CallManager Integrated Mailbox Configuration, page 31-4
- Securing the Voice-Mail Port, page 31-4
- Cisco Unity Configuration Checklist, page 31-5
- Where to Find More Information, page 31-7

System Requirements

The following lists provide requirements for your phone system and the Cisco Unity server. For specific version information, refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity.*

Phone System

- A Cisco Unified Communications applications server that consists of Cisco Unified CallManager software that is running on a Cisco Media Convergence Server (MCS) or customer-provided server that meets approved Cisco configuration standards

- Cisco licenses for all phone lines, IP phones, and other H.323-compliant devices or software (such as Cisco Virtual Phone and Microsoft NetMeeting clients) that will be connected to the network, as well as one license for each Cisco Unity port
- IP phones for the Cisco Unified CallManager extensions
- A LAN connection in each location where you will plug an IP phone into the network
- For multiple Cisco Unified CallManager clusters, subscribers can dial an extension on another Cisco Unified CallManager cluster without having to dial a trunk access code or prefix.

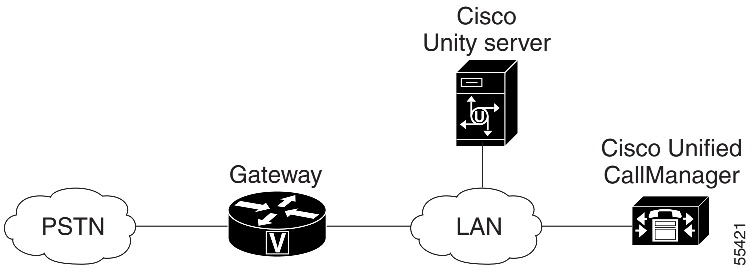
Cisco Unity Server

- Cisco Unity system that was installed and made ready for the integration as described in the *Cisco Unity Installation Guide*.
- The applicable Cisco Unity-CM TSP installed. For more information on compatible versions of the TSP, refer to the *Compatibility Matrix: Cisco Unity Connection*, the *Cisco Unity-CM TSP*, and the Cisco Unified CallManager Express documentation.
- A license that enables the appropriate number of voice-messaging ports.

Integration Description

The integration uses the LAN to connect Cisco Unity and Cisco Unified CallManager. The gateway provides connections to the PSTN. Figure 31-1 shows the connections.

Figure 31-1 Connections Between the Phone System and Cisco Unity



Note The following example applies only if the caller goes through the Cisco Unity Auto Attendant. Most other calls are routed directly to the correct voice mailbox. For example, callers who call a subscriber and get forwarded to voice mail go directly to the voice mailbox and can record a voice message. Subscribers who call in to check their voice messages from their own phones, go directly to their voice mailbox and can listen to voice messages.

1. When an external call arrives, the Cisco gateway sends the call over the LAN to the machine on which Cisco Unified CallManager is installed.
2. For Cisco Unified CallManager lines that are configured to route calls to Cisco Unity, Cisco Unified CallManager routes the call to an available Cisco Unity extension.
3. Cisco Unity answers the call and plays the opening greeting.
4. During the opening greeting, the caller enters either the name of a subscriber or an extension; for example, 1234.

5. Cisco Unity notifies Cisco Unified CallManager that it has a call for extension 1234.
6. At this point, the path of the call depends on whether Cisco Unity is set up to perform supervised transfers or release transfers. Refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.0* for more information.

Cisco Unified CallManager SIP Trunk Integration

Cisco Unity Connection 1.1 supports a SIP trunk integration with the Cisco Unified CallManager phone system when the Cisco Unified CallManager phone system has only SIP phones. Refer to the *Cisco Unified CallManager 5.0 SIP Trunk Integration Guide for Cisco Unity Connection* for more detailed information. The following list describes a few tips that should be performed from the Cisco Unified CallManager Administration side when integrating the Cisco Unified CallManager phone system with Cisco Unity Connection by a SIP trunk:

- Create a SIP trunk that points to Cisco Unity 4.2 and ensure that "Redirecting Number IE Delivery - Outbound" is checked. This instructs Cisco Unified CallManager to send the Diversion Header to Cisco Unity, so you access the correct voice mailbox. Refer to "Trunk Configuration" in the *Cisco Unified CallManager Administration Guide*.

Note Cisco Unified CallManager SIP trunk integration applies to MWI. When you configure the SIP trunk security profile for the SIP voice-messaging trunk, check "Accept Unsolicited Notification." This ensures that MWI will operate properly. You must enable "Accept Header Replacement" if you want to support transfers. This allows "REFER w/replaces" to be passed, which is used for Cisco Unity-initiated, supervised transfers.

- Assure that your phones support DTMF Relay as per RFC-2833. Cisco Unity will support both OOB and RFC-2833. For more information on compatible versions of the TSP, refer to the *Compatibility Matrix: Cisco Unity Connection*, the *Cisco Unity-CM TSP*, and the Cisco Unified CallManager Express documentation.
- Define a route pattern (for example, 7555) and point that route pattern to the SIP trunk to Cisco Unity. Refer to "Route Pattern Configuration" in the *Cisco Unified CallManager Administration Guide*.
- Define a voice mail pilot (for example, 7555). Refer to "Cisco Voice-Mail Pilot Configuration" in the *Cisco Unified CallManager Administration Guide*.
- Define a voice mail profile (for example, VM Profile 1) with the voice mail pilot that you defined in the previous step. Refer to "Voice-Mail Profile Configuration" in the *Cisco Unified CallManager Administration Guide*.

Note Make the voice mail profile that you defined in the last step the system default.

Cisco Unity Cisco Unified CallManager Integrated Mailbox Configuration

When Cisco Unified CallManager release 5.0 integrates with Cisco Unity version 4.0(4) (or later) with Microsoft Exchange, Cisco Unified CallManager administrators can create Cisco Unity subscriber voice mailboxes, one at a time, from the Directory Number Configuration or End User Configuration windows.

Note For information on Cisco Unified CallManager integration with Cisco Unity Connection, refer to the *Cisco Unified CallManager 5.0 SCCP Integration Guide for Cisco Unity Connection 1.1* or the *Cisco Unified CallManager 5.0 SIP Trunk Integration Guide for Cisco Unity Connection 1.1*.

Requirements

- Cisco Unified CallManager release 5.0(x)
- Cisco Unity release 4.0(4) or later with Microsoft Exchange
- Cisco Unified CallManager Integrated Voice Mailbox asp page (installed on the Cisco Unified CallManager server from the Cisco Unity server)
- RIS Data Collector service that is activated on Cisco Unified CallManager server

Restrictions

- After a mailbox is created, no automatic synchronization of mailbox data happens between Cisco Unity and Cisco Unified CallManager. All changes get synchronized manually on both systems.
- The system does not support creation of Internet, VPIM, AMIS, Bridge, or Domino subscriber mailboxes from Cisco Unified CallManager Administration.
- The system does not support bulk or batch import of Cisco Unity mailboxes by using the Bulk Administration Tool (BAT).
- Creation of Cisco Unity mailbox creates a Cisco Unity subscriber account directly in SQL, so new subscribers can be viewed and updated on the Cisco Unity Administrator when the create mailbox transaction completes.
- A log file records Cisco Unity mailbox transactions that are made by using Cisco Unified CallManager Administration on the Cisco Unity server.
- The system writes associated diagnostic logs to a log file.
- Audit log and diagnostic files do not record the transmission of credentials across the network.

Securing the Voice-Mail Port

When you configure security for Cisco Unified CallManager voice mail ports and Cisco Unity SCCP devices, a TLS connection (handshake) opens for authenticated devices after each device accepts the certificate of the other device; likewise, the system sends SRTP streams between devices; that is, if you configure the devices for encryption.

When the device security mode equals authenticated or encrypted, the Cisco Unity-Unified CMTSP connects to Cisco Unified CallManager through the Cisco Unified CallManager TLS port. When the security mode equals non-secure, the Cisco Unity TSP connects to Cisco Unified CallManager through the Cisco Unified CallManager port.

For interactions, restrictions, and procedures on how to configure security, refer to the *Cisco Unified CallManager Security Guide*.

Cisco Unity Configuration Checklist

Table 31-1 provides steps to configure the Cisco Unity voice-messaging system.

Table 31-1 Cisco Unity Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Ensure that you have met the system requirements for Cisco Unified CallManager and Cisco Unity.	System Requirements, page 31-1 *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity*
Step 2	Add voice-mail ports (directory numbers) for each port that you are connecting to Cisco Unity.	Cisco Voice-Mail Port Configuration, *Cisco Unified CallManager Administration Guide* *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity*
Step 3	Add a voice-mail pilot number for the voice-mail ports.	Cisco Voice-Mail Pilot Configuration, *Cisco Unified CallManager Administration Guide* *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity*
Step 4	Specify MWI and voice-mail extensions.	Service Parameters Configuration, *Cisco Unified CallManager Administration Guide* Message Waiting Configuration, *Cisco Unified CallManager Administration Guide* *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity*
Step 5	Add the Voice Mail Port DNs to a line group.	Configuring a Line Group, *Cisco Unified CallManager Administration*
Step 6	Add the line group that contains the Voice Mail Port DNs to a hunt list.	Adding a Route List, *Cisco Unified CallManager Administration*
Step 7	Associate the hunt list that contains the line group with a hunt pilot. **Note** The hunt pilot must match the voice-mail pilot that is configured and used by the voice-mail profiles.	Configuring a Route Pattern, *Cisco Unified CallManager Administration Guide*
Step 8	Set up the voice-mail pilot number.	Cisco Voice-Mail Pilot Configuration, *Cisco Unified CallManager Administration Guide*

Table 31-1 Cisco Unity Configuration Checklist (continued)

Configuration Steps		**Procedures and Related Topics**
Step 9	Set up the voice-mail profile.	Voice-Mail Profile Configuration, *Cisco Unified CallManager Administration Guide* *Cisco Unified CallManager Integration Guide for Cisco Unity*
Step 10	Set up the voice-mail service parameters.	Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*. *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity*
Step 11	Enable the DTMF relay feature in the gateways.	*Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity*
Step 12	Install, configure, and test the TAPI service provider [for Cisco Unity 3.1(x) and earlier].	
Step 13	Configure Cisco Unity for the integration [for Cisco Unity 3.1(x) and earlier]. For multiple clusters of Cisco Unified CallManager, set up MWI ports. Create a new integration between Cisco Unity and Cisco Unified CallManager.	Message Waiting Configuration, *Cisco Unified CallManager Administration Guide*
Step 14	Set up Cisco Unified CallManager authentication and encryption (Cisco Unity 4.0(5) and later).	*Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity* *Cisco Unified CallManager Security Guide*
Step 15	Test the integration.	*Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity* *Cisco Unity Troubleshooting Guide* Refer to the installation guide for the phone system.
Step 16	Integrate the secondary server for Cisco Unity failover (use when Cisco Unity failover is installed).	*Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity* *Cisco Unity Failover Guide*
Step 17	Configure an application user. **Note** You must use the same user name and password that you defined in Cisco Unity Administrator.	Application User Configuration, *Cisco Unified CallManager Administration Guide* *Cisco Unified CallManager Installation Guide for Cisco Unity*

Table 31-1 Cisco Unity Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 18	Choose the auto-generated Cisco Unity server in the Application Server Configuration window in Cisco Unified CallManager Administration. **Note** For application user, choose the application user you created in Step 17.	Application Server Configuration, *Cisco Unified CallManager Administration Guide*
Step 19	If using Cisco Unified CallManager Administration to configure voice mail subscribers, perform the following steps [requires Cisco Unity 4.0(4) or later]: • Copy the voicemailbox.asp file to the Cisco Unified CallManager server. • Set up the Cisco Unity Cisco Unified CallManager Integrated Mailbox Configuration administrator account. (You must perform this step for the failover server if subscribers will be created on the failover server.) • Create a Cisco Unity voice mailbox. **Note** You must configure both Cisco Unity and Cisco Unified CallManager Administration (for example, set up Cisco Unity voice mailbox templates, Cisco Unified CallManager dial plans) to create voice mailboxes.	*Cisco Unified CallManager Installation Guide for Cisco Unity* *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity* Directory Number Configuration, *Cisco Unified CallManager Administration Guide* End User Configuration, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Additional Cisco Documentation

- Cisco Voice-Mail Port Configuration, *Cisco Unified CallManager Administration Guide*
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
- Directory Number Configuration, *Cisco Unified CallManager Administration Guide*
- End User Configuration, *Cisco Unified CallManager Administration Guide*
- Application User Configuration, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity*
- *Cisco Unified CallManager 5.0 SIP Trunk Integration Guide for Cisco Unity Connection*
- *Cisco Unity Installation Guide*
- *Cisco Unity Troubleshooting Guide*

Cisco DPA Integration

The Cisco DPA 7630 and 7610 Voice Mail Gateways (DPA 7630/7610) enable you to integrate Cisco Unified CallManager systems with Octel voice-mail systems, which might also connect to either Definity or Meridian 1 PBX systems. This integration enables you to use your existing third-party telephony systems along with your Cisco IP telephony system.

For example, you can ensure that features such as message-waiting indicators (MWI) for Octel voice messages are properly set on Cisco Unified IP Phones (connected to Cisco Unified CallManager) and traditional telephony phones (connected to Definity or Meridian 1 PBX systems).

Using the DPA 7630/7610, you can integrate the following systems:

- Cisco CallManager 3.1(1) or higher
- Octel 200 and 300 voice-messaging systems (using APIC/NPIC integration)
- Octel 250 and 350 voice-messaging systems (using FLT-A/FLT-N integration)
- Definity G3 PBX systems (DPA 7630 only)
- Meridian 1 PBX systems (DPA 7610 only)

These sections provide you with an overview of the DPA 7630/7610 and its interactions with the other components in traditional and IP telephony networks:

- Understanding the DPA 7630/7610, page 32-1
- How the DPA 7630/7610 Works, page 32-2

Understanding the DPA 7630/7610

The DPA 7630/7610 functions as a gateway between Cisco Unified CallManager and an Octel system (which may connect to a PBX system), and performs these tasks:

- Determines the call type from Cisco Unified CallManager and sends display, light, and ring messages to the Octel system.
- Determines when the Octel system is attempting to transfer, set message waiting indicators (MWI) and so on, and sends the appropriate messages to Cisco Unified CallManager.
- Converts dual-tone multi frequency (DTMF) tones to Skinny Client Control Protocol messages.
- Provides companding-law transcoding and voice compression.
- Performs Real-Time Transport Protocol (RTP) encapsulation of the voice message.

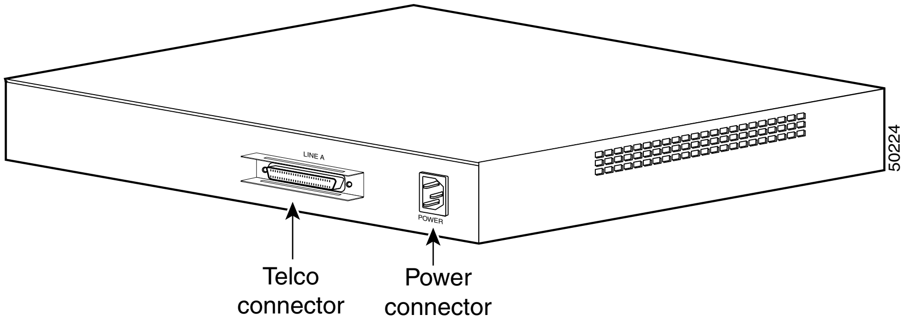
How the DPA 7630/7610 Works

With the Cisco DPA 7630/7610, you can integrate your existing Octel voice-mail system with Cisco Unified CallManager and either a Definity PBX system or a Meridian 1 PBX system. If you have a Definity PBX, use the DPA 7630; if you have a Meridian 1 system, use the DPA 7610.

The DPA 7630/7610 functions by emulating digital phone or PBX systems. This capability allows it to appear like these devices to Cisco Unified CallManager, Octel, Definity, and Meridian 1 systems.

Figure 32-1 illustrates the Cisco DPA.

Figure 32-1 Cisco DPA



Why is the DPA 7630/7610 Needed?

If you want to migrate your telephony system from a Definity G3 PBX or a Meridian 1 PBX to Cisco Unified CallManager, you must decide whether to do a complete cutover to Cisco Unified CallManager or to migrate slowly. If you do a complete cutover to Cisco Unified CallManager and Cisco voice-mail solution, you do not need the DPA 7630/7610. However, if you are slowly migrating your systems, you might want to maintain some phones on the Definity or Meridian 1 PBX while you are installing new phones on the Cisco Unified CallManager system. You might want to use your existing Octel voice-mail system with your Cisco Unified CallManager system. In these cases, the DPA 7630/7610 can assist your migration to Cisco Unified CallManager.

Can I Just Use SMDI?

The fact is voice mail systems such as Octel were designed to integrate to only one PBX at a time presents one difficulty with migration. To resolve this difficulty, many people use Simplified Message Desk Interface (SMDI), which was designed to enable integrated voice-mail services to multiple clients.

To use SMDI, you must ensure that your voice-mail system meets several qualifications:

- It must have sufficient database capacity to support two PBX systems simultaneously and to associate each mailbox with the correct PBX to send MWI information on the correct link.

- It must be possible to physically connect the IP network to the voice-messaging system while maintaining the existing physical link to the PBX.
- It must support analog integration. SMDI primarily acts as an analog technology.

Additionally, SMDI requires reconfiguration of your existing telephony network.

What If I Cannot Use SMDI?

SMDI might not be an option for you, particularly if you are using a digital interface on your Octel systems. Octel systems with digital line cards emulate digital phones, and appears to the PBX as digital extensions, referred to as per-port or PBX integration cards (PIC). On PIC systems, the voice and data streams (for setting MWI) use the same path. The system sets and clears the MWIs via feature access codes on dedicated ports. Because these PIC ports use proprietary interfaces, you cannot use standard interfaces to connect them to the Cisco Unified CallManager system.

The DPA 7630/7610 can, however, translate these interfaces to enable communication among the Cisco Unified CallManager, Octel, and Definity or Meridian 1 systems. Depending on the needs of your network, you can choose among several different integration methods.

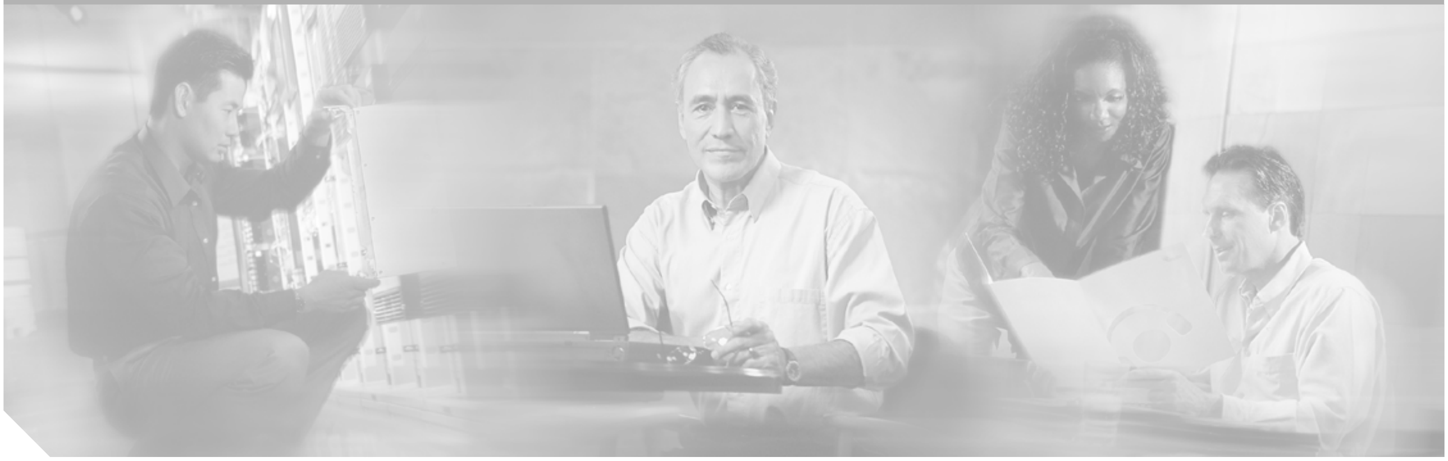
Where to Find More Information

Related Topic

- SMDI Voice Mail Integration, page 30-1

Additional Cisco Documentation

- *Cisco DPA 7630/7610 Voice Mail Gateways Administration Guide*



PART 7

System Features

Call Park

The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the system. For example, 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. Someone on another phone in your system can then dial the call park extension to retrieve the call.

For more information about call park, see Call Park in the *Cisco Unified CallManager Features and Services Guide*.

CHAPTER 34

Call Pickup Group

The Call Pickup Group feature allows users to answer calls that come in on a directory number other than their own. For more information about call pickup group, see Call Pickup Group in the *Cisco Unified CallManager Features and Services Guide*.

CHAPTER 35

Cisco Unified IP Phone Services

System administrators use Cisco Unified IP Phone Services Configuration, a menu option in Cisco Unified CallManager Administration, to define and maintain the list of Cisco Unified IP Phone services to which users can subscribe at their site. Cisco Unified IP Phone services include Extensible Markup Language (XML) applications that enable the display of interactive content with text and graphics on Cisco Unified IP Phones.

Note Cisco Unified IP Phone services supports Cisco Unified IP Phone Models 7970, 7960, 7940, 7912, and 7905.

After the list of services is configured, users can log in to the Cisco Unified CallManager User Options Menu and subscribe to these services for their Cisco Unified IP Phones, or an administrator can add services to Cisco Unified IP Phones and device profiles. Administrators can assign services to speed-dial buttons, so users have one-button access to the services.

Cisco Unified CallManager provides sample Cisco Unified IP Phone services applications through the developer web site. You can also create customized Cisco Unified IP Phone applications for your site.

This section covers the following topics:

- Understanding Cisco Unified IP Phone Services, page 35-1
- Guidelines and Tips, page 35-2
- Dependency Records, page 35-3
- Cisco Unified IP Phone Service Configuration Checklist, page 35-3
- Where to Find More Information, page 35-4

Understanding Cisco Unified IP Phone Services

Cisco Unified IP Phone services comprise XML applications that enable the display of interactive content with text and graphics on Cisco Unified IP Phones.

Note Cisco Unified IP Phone services support Cisco Unified IP Phone Models 7970, 7960, 7940, 7912, and 7905.

A user can access a service from the supported phone model in two ways. The user can press the button labeled “services,” or user can use a preconfigured phone button. When the user presses the services button, the phone uses its HTTP client to load a specific URL that contains a menu of services to which the user has subscribed for the phone. The user then chooses a service from the listing. When a service is chosen from the menu, the URL gets requested via HTTP, and a server provides the content, which then updates the phone display. When the user presses the phone button that is configured for a service, the URL gets requested via HTTP.

Typical services that might be supplied to a phone include weather information, stock quotes, and news quotes. Deployment of Cisco Unified IP Phone Services occurs using the HTTP protocol from standard web servers, such as the Microsoft Internet Information Server (IIS).

Users can only subscribe to services that are configured through Cisco Unified CallManager Administration. The following list gives information that is configured for each service:

- URL of the server that provides the content
- Service name and description, which help end users browsing the system
- A list of parameters that are appended to the URL when it is sent to the server

  These parameters personalize a service for an individual user. Examples of parameters include stock ticker symbols, city names, zip codes, or user IDs.

From Cisco Unified CallManager Administration, you can subscribe a lobby phone or other shared devices to a service.

After the system administrator configures the services, users can log in to the Cisco Unified IP Phone User Options and subscribe to services. From the Cisco Unified IP Phone User Options, users can

- Subscribe to any service on their phone (Subscriptions occur on a per-device basis.)
- Add and update the service URL button

You can also subscribe to services from Cisco Unified CallManager Administration and from the Bulk Administration Tool (BAT) application.

When the user clicks the Subscribe button, Cisco Unified CallManager builds a custom URL and stores it in the database for this subscription. The service then appears on the device services list.

Guidelines and Tips

A Cisco Unified IP Phone displays graphics or text menus, depending on how the services are configured.

The Cisco Unified IP Phone Model 7960 supports the HTTP header that is sent with any window that includes a Refresh setting. Therefore, a new window can, after a fixed time, replace any XML object that displays. The user can force a reload by quickly pressing the Update softkey. If a timer parameter of zero was sent in the header, the window only moves to the next window when you press the Update softkey. The window never automatically reloads.

The Cisco Unified IP Phone Model 7960 supports the following softkeys that are intended to help the data entry process:

- Submit—This softkey indicates that the form is complete and that the resulting URL should be sent via HTTP.
- <<—Use the backspace softkey to backspace within a field.
- Cancel—This softkey cancels the current input.

Use the vertical scroll button for field-to-field navigation.

Caution Do not put Cisco Unified IP Phone Services on any Cisco Unified CallManager server at your site or any server that is associated with Cisco Unified CallManager, such as the TFTP server or directory database publisher server. This precaution eliminates the possibility that errors in a Cisco Unified IP Phone Service application will have an impact on Cisco Unified CallManager performance or interrupt call-processing services.

Dependency Records

To find devices that a specific Cisco Unified IP Phone service is using, in the Cisco Unified CallManager Administration Cisco Unified IP Phone Services Configuration window, choose Dependency Records from the Related Links drop-down list box and click **Go**. The Dependency Records Summary window displays information about devices that are using the Cisco Unified IP Phone Service. To find out more information about the device, 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 and Cisco Unified IP Phone Services Configuration in the *Cisco Unified CallManager Administration Guide*.

Cisco Unified IP Phone Service Configuration Checklist

Table 35-1 provides a checklist to configure Cisco Unified IP Phone service.

Table 35-1 Cisco Unified IP Phone Service Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure Cisco Unified IP Phone Services to the system. Each service includes a name, description, and URL, which helps users who are browsing the system.	Configuring a Cisco Unified IP Phone Service, *Cisco Unified CallManager Administration Guide*
Step 2	Configure the list of parameters that are used to personalize a service for an individual user.	Configuring a Cisco Unified IP Phone Service Parameter, *Cisco Unified CallManager Administration Guide*
Step 3	Create and customize a phone button template that includes the service URL button; then, assign the IP phone service to the service URL button.	Configuring Phone Button Templates, *Cisco Unified CallManager Administration Guide* Adding a Cisco Unified IP Phone Service to a Phone Button, *Cisco Unified CallManager Administration Guide*
Step 4	Notify users that the Cisco Unified IP Phone Service feature is available.	Refer to the phone documentation for instructions on how users access Cisco Unified IP Phone services.

Where to Find More Information

Related Topics

- Phone Button Template Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified IP Phone Services Configuration, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager* (specific to phone model)
- Cisco Unified IP Phone user documentation and release notes (specific to models)

CHAPTER 36

Cisco Extension Mobility and Phone Login Features

The Cisco Extension Mobility feature allows users to configure any Cisco Unified IP Phone 7940 or Cisco Unified IP Phone 7960 as their own, on a temporary basis, by logging in to that phone. After a user logs in, the phone adopts the user individual user default device profile information, including line numbers, speed dials, services links, and other user-specific properties of a phone. For example, when user A occupies a desk and logs in to the phone, that user's directory number(s), services, speed dials, and other properties appear on that phone; but when user B uses the same desk at a different time, user B's information appears. The Cisco Extension Mobility feature dynamically configures a phone according to the current user.

Previously, only administrators could change phone settings through Cisco Unified CallManager Administration. The Cisco Extension Mobility feature allows users to change phone settings themselves without accessing Cisco Unified CallManager Administration. Instead, when users authenticate themselves at the phone, a login service performs the administrative updates.

The programmable login service enforces a variety of uses, including duration limits on phone configuration (persistence) and authorization to log in to a particular phone. A Cisco IP Phone XML service provides the user interface to the login service that is provided in this release.

For more information on how to configure the Cisco Extension Mobility feature, refer to the "Cisco Extension Mobility" chapter in the *Cisco Unified CallManager Features and Services Guide*.

Cisco Unified CallManager Attendant Console

Cisco Unified CallManager Attendant Console, a client-server application, allows you to set up Cisco Unified IP Phones as attendant consoles. Employing a graphical user interface, the attendant console uses 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.

For information and configuration procedures for Cisco Unified CallManager Attendant Console, refer to the "Cisco Unified CallManager Attendant Console" section in the *Cisco Unified CallManager Features and Services Guide*.

Cisco Unified CallManager Assistant

The Cisco Unified CallManager Assistant (Cisco Unified CM Assistant) feature enables managers and their assistants to work together more effectively. Cisco Unified CM Assistant supports two modes of operation: proxy line support and shared line support. Both modes support multiple calls per line for the manager. The Cisco IP Manager Assistant service supports both proxy line and shared line support in a cluster.

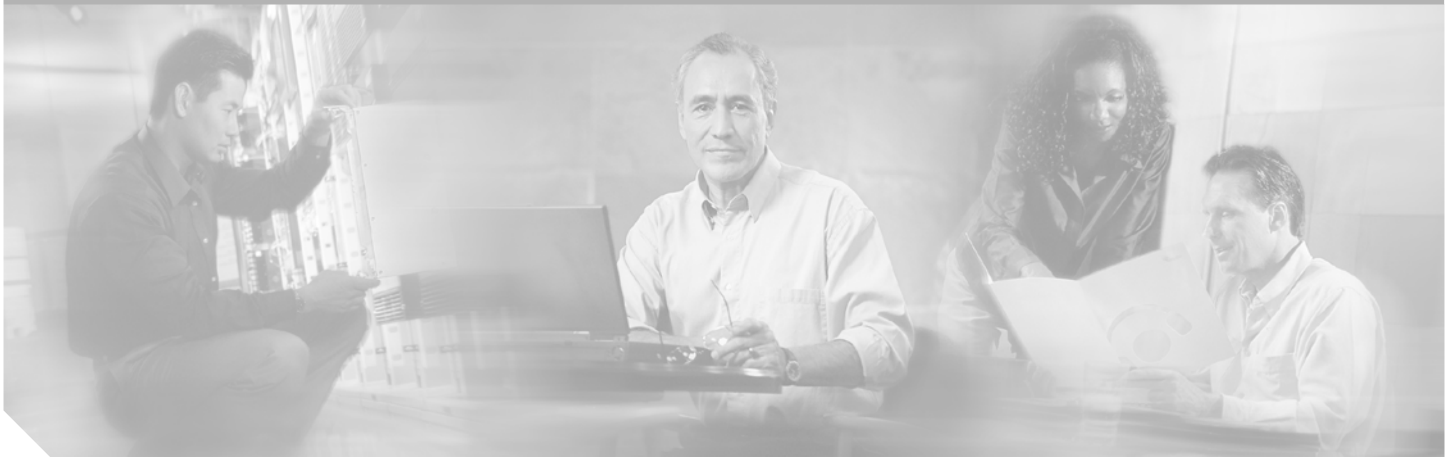
Both modes of Cisco Unified CM Assistant comprise enhancements to phone capabilities for the manager and desktop interfaces that are primarily for the use of the assistant.
Cisco Unified CM Assistant with proxy line support includes a call-routing service.

With Cisco Unified CM Assistant with proxy line support, the service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets based on preconfigured call filters. The manager can change the call routing dynamically; for example, with a softkey press on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Cisco Unified CallManager users comprise managers and assistants. The Cisco Unified CM Assistant with proxy line support routing service intercepts a manager user calls and routes them appropriately (Cisco Unified CM Assistant with shared line support does not support routing). An assistant user handles calls on behalf of a manager. Cisco Unified CM Assistant comprises features for managers and features for assistants.

Related Topics

- Cisco Unified CallManager Assistant With Proxy Line Support, *Cisco Unified CallManager Features and Services Guide*
- Cisco Unified CallManager Assistant With Shared Line Support, *Cisco Unified CallManager Features and Services Guide*



PART 8

Devices and Protocols

CHAPTER 39

Understanding Cisco Unified CallManager Voice Gateways

Cisco Unified Communications gateways enable Cisco Unified CallManager to communicate with non-IP telecommunications devices. Cisco Unified CallManager supports several types of voice gateways.

This section covers the following topics:

- Cisco Voice Gateways, page 39-1
- Gateways, Dial Plans, and Route Groups, page 39-12
- Gateway Failover and Fallback, page 39-13
- Gateway Configuration Checklist, page 39-16
- Where to Find More Information, page 39-18

Cisco Voice Gateways

Cisco Unified CallManager supports several types of Cisco Unified Communications gateways. Gateways use call control protocols to communicate with the PSTN and other non-IP telecommunications devices, such as private branch exchanges (PBXs).

Trunk interfaces specify how the gateway communicates with the PSTN or other external devices by using time-division multiplexing (TDM) signaling. Cisco Unified CallManager and Cisco gateways use a variety of TDM interfaces, but supported TDM interfaces vary by gateway model. Refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)* document for more information about selecting and configuring gateways. The following list gives available interfaces that Cisco Unified CallManager supports:

- Foreign Exchange Office (FXO)
- Foreign Exchange Station (FXS)
- T1 Channel Associated Signaling (CAS)
- Basic Rate Interface (BRI)
- T1 PRI—North American ISDN Primary Rate Interface (PRI)
- E1 PRI—European ISDN Primary Rate Interface (PRI)
- QSIG—Q signaling protocol that is based on ISDN standards
- Session Initiation Protocol (SIP)

Cisco Unified CallManager can use H.323 gateways that support E1 CAS, but you must configure the E1 CAS interface on the gateway.

For information about IP telephony protocols, see the "Understanding IP Telephony Protocols" chapter.

These sections provide an overview of the following gateways that Cisco Unified CallManager supports:

- Standalone Voice Gateways, page 39-2
- Cisco Catalyst 4000 and 6000 Voice Gateway Modules, page 39-5
- H.323 Gateways, page 39-7

Standalone Voice Gateways

This section describes these standalone, application-specific gateway models that are supported for use with Cisco Unified CallManager.

Cisco Voice Gateway 200

The Cisco Unified Communications Voice Gateway (VG200) provides a 10/100BaseT Ethernet port for connection to the data network. The following list gives available telephony connections:

- 1 to 4 FXO ports for connecting to a central office or PBX
- 1 to 4 FXS ports for connecting to POTS telephony devices
- 1 or 2 Digital Access T1 ports for connecting to the PSTN
- 1 or 2 Digital Access PRI ports for connecting to the PSTN
- MGCP or H.323 interface to Cisco Unified CallManager
  - MGCP mode supports T1/E1 PRI, T1 CAS, FXS, FXO. (Only the user side supports BRI.)
  - H.323 mode supports E1/T1 PRI, E1/T1 CAS, FXS, and FXO. H.323 mode supports E&M, fax relay, and G.711 modem.

The MGCP VG200 integration with legacy voice-messaging systems allows the Cisco Unified CallManager to associate a port with a voice mailbox and connection.

Cisco Access Digital Trunk Gateways DT-24+/DE-30+

The Cisco Access Digital Trunk Gateways DT-24+/DE-30+ provide the following features:

- Digital Access PRI (network or user side)
- T1 CAS connections (DT-24+) that support E&M signaling with wink or delay dial supervision
- FXO with loop-start or ground-start circuit emulation
- MGCP interface to Cisco Unified CallManager

Cisco VG248 Analog Phone Gateway

The Cisco VG248 Analog Phone Gateway has a standalone, 19-inch rack-mounted chassis with 48-FXS ports. This product allows on-premise analog telephones, fax machines, modems, voice-messaging systems, and speakerphones to register with a single Cisco Unified CallManager cluster.

Cisco VG248 Analog Phone Connectivity

The Cisco VG248 Analog Phone Gateway communicates with Cisco Unified CallManager by using the Skinny Client Control Protocol to allow support for the following supplementary services features for analog phones:

- Call transfer
- Conference
- Call waiting (with calling party ID display)
- Hold (including switch between parties on hold)
- Music on hold
- Call forward all
- Send all calls to voice-messaging system
- Group call pickup
- Voice-messaging system message waiting indication
- Speed dial (maximum of 9 speed dials)
- Last number redial
- Cisco fax relay
- Dynamic port and device status that is available from Cisco Unified CallManager

Cisco VGC Phone Device Types

All Cisco VG248 ports and units appear as distinct devices in Cisco Unified CallManager with the device type “Cisco VGC Phone.” Cisco Unified CallManager recognizes and configures each port as a phone.

Fax and Modem Connectivity

The Cisco VG248 supports legacy fax machines and modems. When using fax machines, the Cisco VG248 uses either the Cisco fax relay or pass-through/up speed technology to transfer faxes across the network with high reliability.

You can connect any modem to the Cisco VG248 by using pass-through mode.

Voice-Mail Connectivity

The Cisco VG248 generates call information by using the Simplified Message Desk Interface (SMDI) format for all calls that are ringing on any of the 48 analog lines that connect to it. It will also pass on SMDI call information from other Cisco VG248s, or from a legacy PBX, to the voice-messaging system. Any commands for message-waiting indicators get sent to Cisco Unified CallManager and to any other attached SMDI hosts.

This mechanism allows for many new configurations when SMDI-based voice-messaging systems are used, including

- You can share a single voice-messaging system between Cisco Unified CallManager and a legacy PBX.
- Voice-messaging system and Cisco VG248 can function remotely in a centralized call-processing model.
- Multiple clusters can use a single voice-messaging system, by using one Cisco VG248 per cluster.
- Configure multiple voice-messaging systems in a single cluster because the Cisco VG248 generates SMDI call information rather than the Cisco Unified CallManager.

Cisco VG248 Time Device

The Cisco VG248 contains a real-time clock that is persistent across power cycles and restarts. The real-time clock gets set for the first time when the device registers with Cisco Unified CallManager. The clock gets set by using the DefineDateTime Skinny message that Cisco Unified CallManager sends. After a power cycle or restart, the clock resets when the Cisco VG248 receives the DefineDateTime message from Cisco Unified CallManager and then resets no more than once per hour thereafter.

Cisco VG248 Configuration File Updates

The Cisco VG248 queries the TFTP server to access the configuration files for the device. The configuration files update whenever you modify the configuration of the Cisco VG248 via Cisco Unified CallManager.

Refer to the Gateway Configuration section and the Cisco Unified IP Phone Configuration section of the *Cisco Unified CallManager Administration Guide* and to the *Cisco VG248 Analog Phone Gateway Software Configuration Guide* for more information.

Cisco VG224 Analog Phone Gateway

The Cisco VG224 Analog Phone Gateway has a standalone, 17-inch rack-mounted chassis with 24-FXS ports. This product allows on-premise analog telephones, fax machines, modems, and speaker phones to register with Cisco Unified CallManager.

This gateway supports the SCCP and SIP protocols.

Cisco IAD2400 Series Integrated Access Device

The Cisco IAD2420 integrated access device provides voice, data, and video services over internet protocol (IP) and asynchronous transfer mode (ATM) networks. By using the Cisco IAD 2420, service providers can deliver toll-quality voice and data services over circuit- or packet-switched networks. The Cisco IAD2420 provides an MGCP interface with Cisco Unified CallManager and supports the following capabilities:

- Analog: FXS ports for POTS telephony devices, FXO ports for PSTN connections
- Digital: Digital Access PRI and Digital Access T1 services

MGCP BRI Call Connections

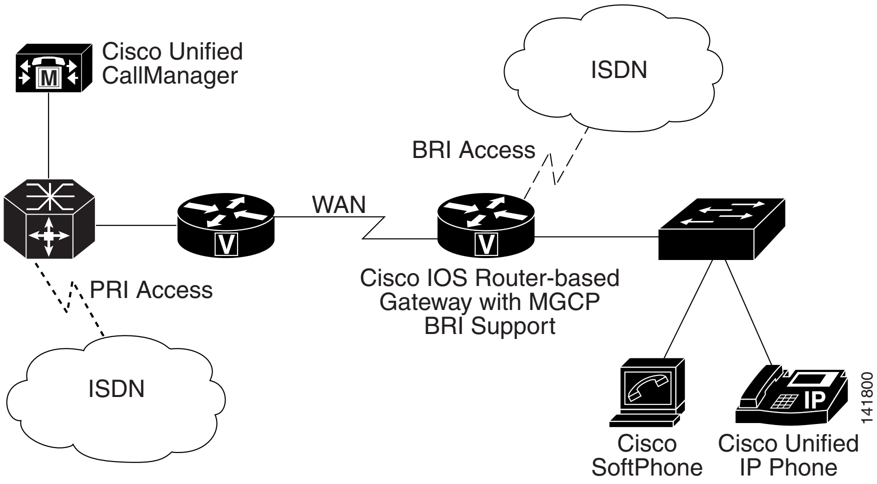
Previously, gateways used H.323 signaling to Cisco Unified CallManager to provide interfaces to the public switched telephone network (PSTN) for BRI ISDN connections. The following list gives drawbacks to using the H.323 protocol:

- Deploying and managing a large number of gateways in a private network represents a very time-consuming task because you must provision every H.323 gateway and its dial plan at the gateway.
- Voice clipping occurs when calls to IP phones use the H.323 gateway because the media cut-through times are very high.
- Calls disconnect if the controlling Cisco Unified CallManager fails during a call.

Now, Cisco Unified CallManager can use a Media Gateway Control Protocol (MGCP) gateway to handle BRI ISDN connections to the PSTN and to provide a centrally administered gateway interface. Cisco Unified CallManager uses logical connections to exchange MGCP and ISDN Q.931 messages with the gateway. This connection uses a User Datagram Protocol (UDP) logical connection for exchanging MGCP messages and a Transmission Control Protocol (TCP) connection for the backhaul ISDN Q.931 messages.

Figure 39-1 shows a typical scenario that centralizes call processing for remote-site BRI trunk gateways that connect to the PSTN. When a call arrives from or goes to the PSTN over the BRI trunk, the Cisco Unified CallManager and the gateway (based on an IOS router) exchange ISDN Q.931 messages across the WAN.

Figure 39-1 Topology Shows a Scenario by Using MGCP BRI Interfaces



For more information about MGCP BRI with Cisco Unified CallManager, refer to the *MGCP-Controlled Backhaul of BRI Signaling in Conjunction with* Cisco Unified CallManager document on the Cisco.com website.

Note The BRI gateway supports MGCP BRI backhaul for BRI trunk only. It does not support BRI phone or station. The IOS gateway supports BRI phones that use Skinny Client Control Protocol.

Cisco Catalyst 4000 and 6000 Voice Gateway Modules

Several telephony modules for the Cisco Catalyst 4000 and 6000 family switches act as telephony gateways. You can use existing Cisco Catalyst 4000 or 6000 family devices to implement IP telephony in your network by using the following voice gateway modules:

- Install Catalyst 6000 voice gateway modules that are line cards in any Cisco Catalyst 6000 or 6500 series switch.
- Install the Catalyst 4000 access gateway module in any Catalyst 4000 or 4500 series switch.

Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module

The Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Modules provide the following features:

- 8 ports for providing
  - Digital T1/E1 connectivity to the PSTN (T1/E1 PRI or T1 CAS with the same features as DT-24+/DE-30+)
  - Digital signal processor (DSP) resources for transcoding and conferencing
- MGCP interface to Cisco Unified CallManager
- Connection to a voice-messaging system (using T1 CAS)

Users have the flexibility to use ports on a T1 module for T1 connections or as network resources for voice services. Similarly, the E1 module provides ports for E1 connections or as network resources. The ports can serve as T1/E1 interfaces, or the ports will support transcoding or conferencing.

Note Either module supports DSP features on any port, but T1 modules cannot be configured for E1 ports, and E1 modules cannot be configured for T1 ports.

Similar to the Cisco MGCP-controlled gateways with FXS ports, the Cisco 6608 T1 CAS gateway supports hookflash transfer. Hookflash transfer defines a signaling procedure that allows a device, such as a voice-messaging system, to transfer to another destination. While the device is connected to Cisco Unified CallManager through a T1 CAS gateway, the device performs a hookflash procedure to transfer the call to another destination. Cisco Unified CallManager responds to the hookflash by using a blind transfer to move the call. When the call transfer completes, the voice channel that connected the original call to the device gets released.

Note Only E&M T1 ports support hookflash transfer.

Cisco Catalyst 6000 24 Port FXS Analog Interface Module

The Cisco Catalyst 6000 24 Port FXS Analog Interface Module provides the following features:

- 24 Port RJ-21 FXS module
- V.34/V.90 modem, voice-messaging system, IVR, POTS
- Cisco fax relay
- MGCP interface to Cisco Unified CallManager

The Catalyst 6000 24 Port FXS Analog Interface Module provides 24 FXS ports for connecting to analog phones, conference room speakerphones, and fax machines. You can also connect to legacy voice-messaging systems by using SMDI and by associating the ports with voice-messaging extensions.

The FXS module provides legacy analog devices with connectivity into the IP network. Analog devices can use the IP network infrastructure for toll-bypass applications and to communicate with devices such as SCCP IP phones and H.323 end stations. The FXS module also supports fax relay, which enables compressed fax transmission over the IP WAN and preserves valuable WAN bandwidth for other data applications.

Cisco Communication Media Module

The Cisco Communication Media Module (CMM), which is a Catalyst 6500 line card, provides T1 and E1 gateways that allow organizations to connect their existing TDM network to their IP communications network. The Cisco CMM provides connectivity to the PSTN also. You can configure the Cisco CMM, which provides an MGCP interface to Cisco Unified CallManager, with the following interface and service modules:

- 6-port T1 interface module for connecting to the PSTN or a PBX
- 6-port E1 interface module for connecting to the PSTN or a PBX
- 24-port FXS interface module for connecting to POTS telephony devices

Cisco Catalyst 4000 Access Gateway Module

The Cisco Catalyst 4000 Access Gateway Module provides an MGCP or H.323 gateway interface to Cisco Unified CallManager. You can configure this module with the following interface and service modules:

- 6 ports for FXS and FXO
- 2 T1/E1 ports for Digital Access PRI and Digital Access T1

Cisco Catalyst 4224 Voice Gateway Switch

The Cisco Catalyst 4224 Voice Gateway Switch provides a single-box solution for small branch offices. The Catalyst 4224 provides switching, IP routing, and PSTN voice-gateway services by using onboard digital signal processors (DSPs). The Catalyst 4224 has four slots that you can configure with multiflex voice and WAN interface cards to provide up to 24 ports. These ports can support the following voice capabilities:

- FXS ports for POTS telephony devices
- FXO ports for PSTN connections
- T1 or E1 ports for Digital Access PRI, and Digital Access T1 services

The Cisco Catalyst 4224 Access Gateway Switch provides an MGCP or H.323 interface to Cisco Unified CallManager.

H.323 Gateways

H.323 devices comply with the H.323 communications standards and enable video conferencing over LANs and other packet-switched networks. You can add third-party H.323 devices or other Cisco devices that support H.323 (such as the Cisco 2600 series, 3600 series, or 5300 series gateways).

Cisco IOS H.323 Gateways

Cisco IOS H.323 gateways such as the Cisco 2600, 3600, 1751, 1760, 3810 V3, 7200 7500, AS5300, and VG200 provide full-featured routing capabilities. Refer to the documentation for each of these gateway types for information about supported voice gateway features and configuration.

T.38 Fax Relay

Transporting real-time Group 3 fax documents over internet protocol (IP) uses the International Telecommunications Union Telecommunication Standardization Sector (ITU-T) recommendation T.38 Fax Relay. The T.38 standard defines the IP network protocol that Internet-aware T.38 fax devices and T.38 IP fax gateways use. The T.38 Fax Relay for VoIP H.323 feature provides standards-based, fax relay protocol support for Cisco and other vendor gateways.

The T.38 Fax Relay feature provides a standards-based, fax relay protocol that is available on several Cisco gateways. Because the T.38 Fax Relay protocol is standards based, Cisco gateways and gatekeepers can interoperate with third-party T.38 enabled gateways and gatekeepers in a mixed vendor network that requires real-time fax relay capabilities.

Cisco Unified CallManager handles the T.38 fax call by using a voice connection. When the originating gateway sends a fax, the gateway establishes an initial voice call. The terminating gateway detects the fax tone that the answering fax machine generates. The VoIP H.323 call stack then starts a T.38 mode request by using H.245 procedures. If the opposite end of the call acknowledges the T.38 mode request, the initial audio channel closes, and T.38 Fax Relay channel opens. When the fax transmission finishes, the call disconnects.

Transcoders should be provisioned for use with T.38 Fax Relay either when codec mismatches exist or when fast-connect procedures are employed.

Outbound FastStart Call Connections

Calls that are placed from IP phones over large WAN topologies can experience voice clipping when the called party goes off hook to answer the call. When H.323 trunks or gateways are separated from the Cisco Unified CallManager server, significant delays can occur because of the many H.245 messages that are exchanged when a call is set up.

With the FastStart feature, information that is required to complete a media connection between two parties gets exchanged during the H.225 portion of call setup, and this exchange eliminates the need for H.245 messages. The connection experiences one roundtrip WAN delay during call setup, and the calling party does not receive voice clipping when the called party answers the call.

Cisco Unified CallManager uses media termination points (MTP) for making an H.323 outbound FastStart call. Cisco Unified CallManager starts an outbound FastStart call by allocating an MTP and opening the receive channel. Next, the H.323 Fast Connect procedure sends the SETUP message with a FastStart element to the called endpoint. The FastStart element includes information about the receiving channel for the MTP.

The called endpoint accepts the H.323 Fast Connect procedure by sending a CALL PROCEEDING, PROGRESS, ALERT, or CONNECT message that contains a FastStart element. When Cisco Unified CallManager receives the FastStart element, it connects the media immediately and avoids the delays with the usual exchange of H.245 messages.

The called endpoint can refuse the H.323 Fast Connect procedure by not returning the FastStart element in any of the messages up to and including the CONNECT message. In this case, the Cisco Unified CallManager handles the call as a normal call and uses the MTP for subsequent media cut-through.

The Outbound FastStart feature requires an MTP. If an MTP is not available when the call is set up, the call continues without FastStart and with no supplementary services. If you want all calls to use FastStart only, you can set the service parameter called “Fail call if MTP allocation fails,” which is located in the Cluster Wide Parameters (Device-H323) portion of the service parameters for the Cisco Unified CallManager service. When you set this parameter to True, the system rejects calls when no MTP is available.

Related Topic

H.323 Gateway Configuration Settings, *Cisco Unified CallManager Administration Guide*

Voice Gateway Model Summary

Table 39-1 summarizes Cisco voice gateways that Cisco Unified CallManager supports with information about the gateway control protocols, trunk interfaces, and port types.

Table 39-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Ports

Gateway Model	Gateway Control Protocol	Trunk Interface	Port Types
Cisco IOS Integrated Routers			
Cisco 1751 and Cisco 1760	MGCP	FXS	POTS
		FXO	Loop start or ground start
Cisco 1880	MGCP	FXS	POTS
		FXO	Loop start or ground start
		BRI	Digital Access BRI
		T1/E1 PRI	Digital Access PRI
		T1 CAS	Digital Access T1, Digital Access PRI
Cisco 2801	MGCP	FXS	POTS
	SCCP	FXO	Loop start or ground start
		T1 CAS	Digital Access T1, Digital Access PRI
		T1 PRI	Digital Access T1, Digital Access PRI
		E1 PRI	Digital Access PRI
		BRI	Digital Access BRI
Cisco 2600 series	MGCP, H.323, or SCCP	FXS	POTS
		FXO	Loop start or ground start
		T1/E1 PRI	T1/E1 PRI
		T1 CAS	E&M
	(Only MGCP supports QSIG.)	QSIG (Not all Cisco 2600 series gateways support QSIG. Refer to your gateway documentation.)	T1/E1 PRI MGCP BRI SCCP BRI (including 269x)
Cisco 2811, 2821, 2851	MGCP	T1 CAS	Loop start or ground start
	SCCP	T1 PRI	Digital Access T1, Digital Access PRI
		E1 PRI	Digital Access PRI
		FXS	POTS
		FXO	Loop start or ground start

Table 39-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Ports (continued)

Gateway Model	Gateway Control Protocol	Trunk Interface	Port Types
Cisco 3600 series	MGCP or H.323 (Only MGCP supports QSIG.)	FXS FXO T1/E1 PRI T1 CAS QSIG (Not all Cisco 3600 series gateways support QSIG. Refer to your gateway documentation.)	POTS Loop start or ground start T1/E1 PRI E&M T1/E1 PRI MGCP BRI (364x and 366x only) SCCP BRI (3625 and 3645)
Cisco 3725	MGCP, H.323, or SCCP (Only MGCP supports QSIG.)	FXS (Only supported in SCCP mode) FXO T1/E1 PRI T1 CAS QSIG	POTS Loop start or ground start T1/E1 PRI E&M T1/E1PRI MGCP BRI (Only supported in SCCP mode)
Cisco 3745	MGCP, H.323, or SCCP (Only MGCP supports QSIG.)	FXS (Only supported in SCCP mode) FXO T1/E1 PRI T1 CAS QSIG	POTS Loop start or ground start T1/E1 PRI E&M T1/E1 PRI MGCP BRI (Only supported in SCCP mode)
Cisco 3825, 3845	MGCP	FXS FXO T1 CAS T1 PRI	Loop start or ground start
Cisco 7200	H.323 (H.225)	T1/E1 CAS T1/E1 PRI	T1/E1 CAS T1/E1 PRI
Cisco Standalone Voice Gateways			
Cisco Voice Gateway 200 (VG200)	MGCP or H.323 (Only MGCP supports QSIG.)	FXO FXS T1/E1 PRI T1 CAS QSIG	Loop start or ground start POTS T1/E1 PRI E&M T1/E1 PRI

Table 39-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Ports (continued)

Gateway Model	Gateway Control Protocol	Trunk Interface	Port Types
Cisco Access Digital Trunk Gateway DE-30+	MGCP	E1 PRI	E1 PRI
		QSIG	E1 PRI
Cisco Access Digital Trunk Gateway DT-24+	MGCP	T1 PRI	T1 PRI
		T1 CAS	E&M
		FXO	Loop start or ground start
		QSIG	T1 PRI
Cisco VG248 Analog Phone Gateway	Skinny Client Control Protocol	FXS	POTS
Cisco VG224 Analog Phone Gateway	MGCP or SCCP	FXS	POTS
Cisco IAD2400	MGCP	FXS	POTS
		FXO	Loop start or ground start
		T1 PRI	T1 PRI
		T1 CAS	E&M
		QSIG	T1 PRI
Cisco Catalyst Voice Gateway Modules			
Cisco Catalyst 4000 Access Gateway Module (WS-X4604-GWY)	MGCP or H.323	FXS	POTS
		FXO	Loop start or ground start
		T1 CAS	E&M
		T1/E1 PRI	T1/E1 PRI
	(Only MGCP supports QSIG.)	QSIG	T1/E1 PRI
Cisco Catalyst 4224 Voice Gateway Switch	MGCP or H.323	FXS	POTS
		FXO	Loop start or ground start
		T1/E1 PRI	T1/E1 PRI
		T1 CAS	E&M
	(Only MGCP supports QSIG.)	QSIG	T1/E1 PRI
Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module (WS-X6608-T1) (WS-X6608-E1)	MGCP	T1/E1 PRI	T1/E1 PRI
		T1 CAS	E&M, loop start, ground start
			T1/E1 PRI
		QSIG	

Table 39-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Ports (continued)

Gateway Model	Gateway Control Protocol	Trunk Interface	Port Types
Cisco Catalyst 6000 24-Port FXS Analog Interface Module (WS-X6624-FXS)	MGCP	FXS	POTS
Cisco Communication Media Module (WS-X6600-24FXS) (WS-X6600-6T1) (WS-X6600-6E1)	MGCP	FXS T1 PRI T1 CAS E1 PRI	POTS T1 PRI E&M E1 PRI

Gateways, Dial Plans, and Route Groups

Gateways use dial plans to access or call out to the PSTN, route groups, and group-specific gateways. The different gateways that are used within Cisco Unified Communications Solutions have dial plans that are configured in different places:

- Configure dial plan information for both Skinny and MGCP gateways in the Cisco Unified CallManager.
- Configure dial plans in Cisco Unified CallManager to access the H.323-based Cisco IOS software gateways. Configure dial peers in the H.323-based gateways to pass the call out of the gateway.

The route group points to one or more gateways and can choose the gateways for call routing based on preference. The route group can serve as a trunk group by directing all calls to the primary device and then using the secondary devices when the primary is unavailable. One or more route lists can point to the same route group.

All devices in a given route group share the same characteristics such as path and digit manipulation. Cisco Unified CallManager restricts the gateways that you can include in the same route group and the route groups that you can include in the same route list. For more information about routing, see the "Route Plan Overview" section on page 17-4.

Route groups can perform digit manipulation that will override what was performed in the route pattern. Configuration information that is associated with the gateway defines how the call is actually placed and can override what was configured in the route pattern.

You can configure H.323 trunks, *not* H.323gateways, to be gatekeeper-controlled trunks. This means that before a call is placed to an H.323 device, it must successfully query the gatekeeper. See the "Gatekeeper and Trunk Configuration in Cisco Unified CallManager" section on page 8-9 for more information.

Multiple clusters for inbound and outbound calls can share H.323 trunks, but MGCP and Skinny-based gateways remain dedicated to a single Cisco Unified CallManager cluster.

Related Topics

- Dependency Records for Gateways and their Route Groups and Directory Numbers, page 39-13
- Cisco Voice Gateways, page 39-1

Dependency Records for Gateways and their Route Groups and Directory Numbers

To find route groups or directory numbers that a specific gateway or gateway port is using, click the Dependency Records link that is provided on the Cisco Unified CallManager Administration Gateway Configuration window. The Dependency Records Summary window displays information about route groups and directory numbers that are using the gateway or port. To find out more information about the route group or directory number, click the route group or directory number, 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, Deleting Gateways, and Removing a Directory Number from a Phone in the *Cisco Unified CallManager Administration Guide*.

Related Topics

- Gateways, Dial Plans, and Route Groups, page 39-12
- Cisco Voice Gateways, page 39-1

Gateway Failover and Fallback

This section describes how these Cisco voice gateways handle Cisco Unified CallManager failover and fallback situations. See the following topics:

- MGCP Gateways, page 39-13
- IOS H.323 Gateways, page 39-14
- Cisco VG248 Analog Phone Gateway, page 39-14

MGCP Gateways

To handle Cisco Unified CallManager failover situations, MGCP gateways receive a list of Cisco Unified CallManagers that is arranged according to the Cisco Unified CallManager group and defined for the device pool that is assigned to the gateway. A Cisco Unified CallManager group can contain one, two, or three Cisco Unified CallManagers that are listed in priority order for the gateway to use. If the primary Cisco Unified CallManager in the list fails, the secondary Cisco Unified CallManager gets used. If the primary and secondary Cisco Unified CallManagers fail, the tertiary Cisco Unified CallManager gets used.

Fallback describes the process of recovering a higher priority Cisco Unified CallManager when a gateway fails over to a secondary or tertiary Cisco Unified CallManager. Cisco MGCP gateways periodically take status of higher priority Cisco Unified CallManagers. When a higher priority Cisco Unified CallManager is ready, it gets marked as available again. The gateway reverts to the highest available Cisco Unified CallManager when all calls go idle or within 24 hours, whichever occurs first. The administrator can force a fallback either by stopping the lower priority Cisco Unified CallManager whereby calls get preserved, by restarting the gateway, which preserves calls, or by resetting Cisco Unified CallManager, which terminates calls.

Note Skinny Client Control Protocol (SCCP) gateways handle Cisco Unified CallManager redundancy, failover, and fallback in the same way as MGCP gateways.

IOS H.323 Gateways

Cisco IOS gateways also handle Cisco Unified CallManager failover situations. By using several enhancements to the **dial-peer** and **voice class** commands in Cisco IOS Release 12.1(2)T, Cisco IOS gateways can support redundant Cisco Unified CallManagers. The command, **h225 tcp timeout** *seconds*, specifies the time that it takes for the Cisco IOS gateway to establish an H.225 control connection for H.323 call setup. If the Cisco IOS gateway cannot establish an H.225 connection to the primary Cisco Unified CallManager, it tries a second Cisco Unified CallManager that is defined in another **dial-peer** statement. The Cisco IOS gateway shifts to the **dial-peer** statement with the next highest **preference** setting.

The following example shows the configuration for H.323 gateway failover:

```
interface FastEthernet0/0
   ip address 10.1.1.10 255.255.255.0
dial-peer voice 101 voip
   destination-pattern 1111
   session target ipv4:10.1.1.101
   preference 0
   voice class h323 1
dial-peer voice 102 voip
   destination-pattern 1111
   session target ipv4:10.1.1.102
   preference 1
   voice class h323 1
voice class h323 1
   h225 timeout tcp establish 3
```

Note To simplify troubleshooting and firewall configurations, Cisco recommends that you use the new `voip-gateway voip bind srcaddr` command for forcing H.323 always to use a specific source IP address in call setup. Without this command, the source address that is used in the setup might vary and depends on protocol (RAS, H.225, H.245, or RTP).

Cisco VG248 Analog Phone Gateway

The Cisco VG248 Analog Phone Gateway supports the Skinny Client Control Protocol (SCCP) for clustering and failover.

Transferring Calls Between Gateways

Using Cisco Unified CallManager Administration, you can configure gateways as OnNet (internal) gateways or OffNet (external) gateways by using Gateway Configuration or by setting a clusterwide service parameter. Used in conjunction with the clusterwide service parameter, Block OffNet to OffNet Transfer, the configuration determines whether calls can be transferred over a gateway.

To use the same gateway to route both OnNet and OffNet calls, associate the gateway with two different route patterns. Make one gateway OnNet and the other OffNet with both having the Allow Device Override check box unchecked.

Configuring Transfer Capabilities Using Gateway Configuration

Using Cisco Unified CallManager Administration Gateway Configuration, you can configure a gateway as OffNet or OnNet. The system considers the calls that come to the network through that gateway OffNet or OnNet, respectively. Use the Gateway Configuration window field, Call Classification, to configure the gateway as OffNet, OnNet, or Use System Default. See Table 39-2 for description of these settings.

The Route Pattern Configuration window provides a drop-down list box called Call Classification, which allows you to configure a route pattern as OffNet or OnNet. When Call Classification is set to OffNet and the Allow Device Override check box is unchecked, the system considers the outgoing calls that use this route pattern as OffNet (if configured as OnNet and check box is unchecked, then outgoing calls are considered OnNet).

The same gateway can be used to route both OnNet and OffNet calls by associating the gateway with two different route patterns: one OnNet and the other OffNet, with both having the Allow Device Override check box unchecked. For outgoing calls, the outgoing device setting classifies the call as either OnNet or OffNet by determining whether the Allow Device Override check box is checked.

In route pattern configuration, if the Call Classification is set as OnNet, the Allow Device Override check box is checked, and the route pattern is associated with an OffNet gateway, the system considers the outgoing call OffNet.

Table 39-2 Gateway Configuration Call Classification Settings

Setting Name	Description
OffNet	This setting identifies the gateway as being an external gateway. When a call comes in from a gateway that is configured as OffNet, the outside ring gets sent to the destination device.
OnNet	This setting identifies the gateway as being an internal gateway. When a call comes in from a gateway that is configured as OnNet, the inside ring gets sent to the destination device.
Use System Default	This setting uses the Cisco Unified CallManager clusterwide service parameter Call Classification.

Configuring Transfer Capabilities by Using Call Classification Service Parameter

To configure all gateways to be OffNet (external) or OnNet (internal), perform the following two steps:

1. Use the Cisco Unified CallManager clusterwide service parameter Call Classification.
2. Configure individual gateways to Use System Default in the Call Classification field that is on the Gateway Configuration window.

Blocking Transfer Capabilities by Using Service Parameters

Block transfer provides a way of restricting transfer between external devices, so fraudulent activity gets prevented. You can configure the following devices as OnNet (internal) or OffNet (external) to Cisco Unified CallManager:

- H.323 gateway
- MGCP FXO trunk
- MGCP T1/E1 trunk
- Intercluster trunk
- SIP trunk

If you do not want OffNet calls to be transferred to an external device (one that is configured as OffNet), set the Cisco Unified CallManager clusterwide service parameter, Block OffNet to OffNet Transfer, to True.

If a user tries to transfer a call on an OffNet gateway that is configured as blocked, a message displays on the user phone to indicate that the call cannot be transferred.

Related Topics

- Route Pattern Configuration, *Cisco Unified CallManager Administration Guide*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide*
- Trunk Configuration, *Cisco Unified CallManager Administration Guide*

Gateway Configuration Checklist

Table 39-3 provides an overview of the steps that are required to configure gateways in Cisco Unified CallManager, along with references to related procedures and topics.

Table 39-3 Gateway Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Install and configure the gateway or voice gateway module in the network.	Refer to the installation and configuration documentation for the model of gateway that you are configuring.
Step 2	Gather the information that you need to configure the gateway to operate with Cisco Unified CallManager.	Gateway Configuration Settings, *Cisco Unified CallManager Administration Guide* Port Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 3	On the gateway, perform any required configuration steps.	Refer to the voice feature software configuration documentation or Cisco IOS documentation for the model of gateway that you are configuring.

Table 39-3 Gateway Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 4	Add and configure the gateway in Cisco Unified CallManager Administration.	Adding Gateways to Cisco Unified CallManager, *Cisco Unified CallManager Administration Guide*
Step 5	Add and configure ports on the gateway or add and configure the Cisco VG248 Analog Phone Gateway.	Port Configuration Settings, *Cisco Unified CallManager Administration Guide* Adding a Cisco VG248 Analog Phone Gateway, *Cisco Unified CallManager Administration Guide* Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*
Step 6	For FXS ports, add directory numbers, if appropriate.	Directory Number Configuration Overview, *Cisco Unified CallManager Administration Guide* Directory Number Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 7	Configure the dial plan for the gateway for routing calls out to the PSTN or other destinations. This configuration can include setting up a route group, route list, and route pattern for the Gateway in Cisco Unified CallManager or, for some gateways, configuring the dial plan on the gateway itself.	*Cisco Unified Communications Solution Reference Network Design* *Cisco Unified CallManager Administration Guide*
Step 8	Reset the gateway to apply the configuration settings.	Resetting and Restarting Gateways, *Cisco Unified CallManager Administration Guide*

Tip To get to the default web pages for many gateway devices, you can use the IP address of that gateway. Make your hyperlink url = http://x.x.x.x/, where x.x.x.x is the dot-form IP address of the device. The web page for each gateway contains device information and the real-time status of the gateway.

MGCP BRI Gateway Configuration Checklist

Table 39-4 provides an overview of the steps that are required to configure a BRI gateway in Cisco Unified CallManager, along with references to related procedures and topics.

Table 39-4 MGCP BRI Gateway Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Install and configure the gateway and voice modules in the network.	Refer to the installation and configuration documentation for the model of gateway that you are configuring.
Step 2	Gather the information that you need to configure the gateway to operate with Cisco Unified CallManager and to configure the trunk interface to the PSTN or external non-IP telephony device.	Gateway Configuration Checklist, page 39-16 Adding a BRI Port to an MGCP Gateway, *Cisco Unified CallManager Administration Guide*
Step 3	On the gateway, perform any required configuration steps.	Refer to the voice feature software configuration documentation or Cisco IOS documentation for the model of gateway that you are configuring.
Step 4	Add and configure the gateway in Cisco Unified CallManager Administration.	Gateway Configuration, *Cisco Unified CallManager Administration Guide*
Step 5	Add and configure ports on the gateway.	Gateway Configuration, *Cisco Unified CallManager Administration Guide*
Step 6	Configure the dial plan for the gateway for routing calls out to the PSTN or other destinations. This configuration can include setting up a route group, route list, and route pattern for the gateway in Cisco Unified CallManager or, for some gateways, configuring the dial plan on the gateway itself.	*Cisco Unified CallManager Administration Guide* *Cisco Unified Communications Solution Reference Network Design (SRND)*
Step 7	Reset the gateway to apply the configuration settings.	*Cisco Unified CallManager Administration Guide*

Tip To get to the default web pages for gateway devices, you can use the IP address of that gateway. Make your hyperlink url = http://x.x.x.x/, where x.x.x.x specifies the dot-form IP address of the device. The web page for each gateway contains device information and the real-time status of the gateway.

Where to Find More Information

Related Topics

- Understanding IP Telephony Protocols, page 40-1
- Understanding Cisco Unified CallManager Trunk Types, page 42-1

- Route Plan Overview, page 17-4
- Gatekeepers and Trunks, page 8-6
- Gateway Configuration, *Cisco Unified CallManager Administration Guide*
- Adding Gateways to Cisco Unified CallManager, *Cisco Unified CallManager Administration Guide*
- Gateway Configuration Settings, *Cisco Unified CallManager Administration Guide*
- Port Configuration Settings, *Cisco Unified CallManager Administration Guide*
- Directory Number Configuration Settings, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design*
- *Configuring Cisco Unified Communications Voice Gateways*
- *Implementing Fax Over IP on Cisco Voice Gateways*
- *Cisco VG248 Analog Phone Gateway Software Configuration Guide*
- *Cisco VG248 Analog Phone Gateway Hardware Installation Guide*

CHAPTER 40

Understanding IP Telephony Protocols

Understanding IP Telephony Protocols briefly describes some of the different protocols and their interaction with Cisco Unified CallManager.

This section covers the following topics:

- IP Protocols, page 40-1
- Analog Telephony Protocols, page 40-3
- Digital Telephony Protocols, page 40-5
- Where to Find More Information, page 40-15

IP Protocols

Cisco Unified CallManager performs signaling and call control tasks such as digit analysis, routing, and circuit selection within the PSTN gateway infrastructure. To perform these functions, Cisco Unified CallManager uses industry standard IP protocols including H.323, MGCP, SCCP, and SIP. Use of Cisco Unified CallManager and these protocols gives service providers the capability to seamlessly route voice and data calls between the PSTN and packet networks.

This section discusses the following IP protocols:

- H.323 Protocol, page 40-1
- Media Gateway Control Protocol (MGCP), page 40-2
- Skinny Client Control Protocol (SCCP), page 40-2
- Session Initiation Protocol (SIP), page 40-3

H.323 Protocol

The International Telecommunications Union (ITU) developed the H.323 standard for multimedia communications over packet networks. As such, the H.323 protocol is a proven ITU standard and provides multivendor interoperability. The H.323 protocol specifies all aspects of multimedia application services, signaling, and session control over an underlying packet network. Audio is standard on H.323 networks, but networks can be scaled to include both video and data. The H.323 protocol can be implemented in large enterprise networks or can be deployed over an existing infrastructure, which makes H.323 an affordable solution.

The basic components of the H.323 protocol are terminals, gateways, and gatekeepers (which provide call control to H.323 endpoints). Similar to other protocols, H.323 applies to point-to-point or multipoint sessions. However, compared to MGCP, H.323 requires more configuration on the gateway.

For more information, refer to the following topics:

- "Adding a Cisco IOS H.323 Gateway" section in the *Cisco Unified CallManager Administration Guide*
- Gatekeeper Configuration chapter in the *Cisco Unified CallManager Administration Guide*
- Understanding Cisco Unified CallManager Trunk Types chapter in the *Cisco Unified CallManager System Guide*
- Understanding Cisco Unified CallManager Voice Gateways chapter in the *Cisco Unified CallManager System Guide*
- Trunk Configuration chapter in the *Cisco Unified CallManager Administration Guide*

Media Gateway Control Protocol (MGCP)

MGCP provides Cisco Unified CallManager a powerful, flexible and scalable resource for call control. Cisco Unified CallManager uses MGCP to control media on the telephony interfaces of a remote gateway and also uses MGCP to deliver messages from a remote gateway to appropriate devices.

MGCP enables a call agent (media gateway controller) to remotely control and manage voice and data communication devices at the edge of multiservice IP packet networks. Because of its centralized architecture, MGCP simplifies the configuration and administration of voice gateways and supports multiple (redundant) call agents in a network. MGCP does not provide security mechanisms such as message encryption or authentication.

Using MGCP, Cisco Unified CallManager controls call processing and routing and provides supplementary services to the gateway. The MGCP gateway provides call preservation (the gateway maintains calls during failover and fallback), redundancy, dial-plan simplification (the gateway requires no dial-peer configuration), hookflash transfer, and tone on hold. MGCP-controlled gateways do not require a media termination point (MTP) to enable supplementary services such as hold, transfer, call pickup, and call park. If the MGCP gateway loses contact with its Cisco Unified CallManager, it falls back to using H.323 control to support basic call handling of FXS, FXO, T1 CAS, and T1/E1 PRI interfaces.

For more information, refer to the "Adding a Cisco IOS MGCP Gateway" section in the *Cisco Unified CallManager Administration Guide*.

Related Topics

- H.323 Protocol, page 40-1
- Skinny Client Control Protocol (SCCP), page 40-2
- Session Initiation Protocol (SIP), page 40-3

Skinny Client Control Protocol (SCCP)

SCCP uses Cisco-proprietary messages to communicate between IP devices and Cisco Unified CallManager. SCCP easily coexists in a multiple protocol environment. The Cisco Unified IP Phone is an example of a device that registers and communicates with Cisco Unified CallManager as an SCCP client. During registration, a Cisco Unified IP Phone receives its line and all other configurations from Cisco Unified CallManager. Once it registers, it is notified of new incoming calls and can make outgoing calls. The SCCP protocol is used for VoIP call signaling and enhanced features such as Message Waiting Indication (MWI).

The Cisco VG248 gateway is another example of a device that registers and communicates with Cisco Unified CallManager by using SCCP. For more information, on the Cisco VG248 gateway refer to the "Adding a Cisco VG248 Analog Phone Gateway" section in the *Cisco Unified CallManager Administration Guide.*

Related Topics

- H.323 Protocol, page 40-1
- Media Gateway Control Protocol (MGCP), page 40-2
- Session Initiation Protocol (SIP), page 40-3

Session Initiation Protocol (SIP)

The Internet Engineering Task Force (IETF) developed the SIP standard for multimedia calls over IP. ASCII-based SIP works in client/server relationships as well as in peer-to-peer relationships. SIP uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more end points. Refer to the Understanding Session Initiation Protocol (SIP) chapter for more information on SIP and the interaction between SIP and Cisco Unified CallManager.

Related Topics

- H.323 Protocol, page 40-1
- Media Gateway Control Protocol (MGCP), page 40-2
- Skinny Client Control Protocol (SCCP), page 40-2

Analog Telephony Protocols

Analog telephony signaling, the original signaling protocol, provides the method for connecting or disconnecting calls on analog trunks. By using direct current (DC) over two-wire or four-wire circuits to signal on-hook and off-hook conditions, each analog trunk connects analog endpoints or devices such as a PBX or analog phone.

To provide connections to legacy analog central offices and PBXs, Cisco Unified CallManager uses analog signaling protocols over analog trunks that connect voice gateways to analog endpoints and devices. Cisco Unified CallManager supports these types of analog trunk interfaces:

- Foreign Exchange Office (FXO)—Analog trunks that connect a gateway to a central office (CO) or private branch exchange (PBX).
- Foreign Exchange Station (FXS)—Analog trunks that connect a gateway to plain old telephone service (POTS) device such as analog phones, fax machines, and legacy voice-mail systems.

You can configure loop-start, ground-start, or E&M signaling protocols for FXO and FXS trunk interfaces depending on the gateway model that is selected. You must use the same type of signaling on both ends of the trunk interface to ensure that the calls properly connect. The following sections describe the types of analog signaling protocols that Cisco Unified CallManager supports:

- Loop-Start Signaling, page 40-4
- Ground-Start Signaling, page 40-4

- E&M Signaling, page 40-4
- Channel Associated Signaling (CAS), page 40-5

Loop-Start Signaling

Loop-start signaling sends an off-hook signal that starts a call and an on-hook signal that opens the loop to end the call. Loop-start trunks lack positive disconnect supervision, and users can experience glare when two calls seize the trunk at the same time.

Related Topics

- Ground-Start Signaling, page 40-4
- E&M Signaling, page 40-4
- Channel Associated Signaling (CAS), page 40-5

Ground-Start Signaling

Ground-start signaling provides current detection mechanisms at both ends of the trunk to detect off-hook signals. This mechanism permits endpoints to agree on which end is seizing the trunk before it is seized, and minimizes the chance of glare. Ground start provides positive recognition of connects and disconnects and is the preferred signaling method for PBX connections. Some PBXs do not support ground-start signaling, so then you must use loop-start signaling for the trunk interface.

Related Topics

- Loop-Start Signaling, page 40-4
- E&M Signaling, page 40-4
- Channel Associated Signaling (CAS), page 40-5

E&M Signaling

E&M signaling uses direct current (DC) over two-wire or four-wire circuits to signal to the endpoint or CO switch when a call is in recEive or transMit (E&M) state. E&M signaling uses signals that indicate off-hook and on-hook conditions. When the connection is established, the audio transmission occurs. The E&M signaling type must be the same for both ends of the trunk interface for successful connections. Cisco Unified CallManager supports these types of E&M signaling:

Wink-start signaling—The originating side sends an off-hook signal and waits to receive a wink pulse signal that indicates the receiving end is ready to receive the dialed digits for the call. Wink start is the preferred signaling method because it provides answer supervision. Not all COs and PBXs support wink-start signaling.

Delay-dial signaling—The originating side sends an off-hook signal, waits for a configurable time period, and then checks if the receiving end is on hook. The originating side sends dialed digits when the receiving side is on hook. The delay allows the receiving end to signal when it is ready to receive the call.

Immediate-start signaling—The originating side goes off hook, waits for a finite time period (for example 200 ms), and then sends the dial digits without a ready signal from the receiving end.

Related Topics

- Loop-Start Signaling, page 40-4
- Ground-Start Signaling, page 40-4
- Channel Associated Signaling (CAS), page 40-5

Channel Associated Signaling (CAS)

Channel associated signaling (CAS) sends the on hook and off hook signals as bits within the frames on the same channel as the audio transmission. CAS is often referred to as robbed bit signaling because CAS takes bits from the voice channel for signaling. These signals can include supervision, addressing, and tones such as busy tone or dial tone.

You can use T1 CAS and E1 CAS digital trunk interfaces to connect a Cisco Unified CallManager call to a CO, a PBX, or other analog device.

T1 CAS

The T1 CAS trunk interface uses in-band E&M signaling to carry up to 24 connections on a link. Both ends of the T1 link must specify T1 CAS signaling. Cisco Unified CallManager provides the T1 CAS signaling option when you configure ports on some MGCP and H.323 voice gateways and network modules. For more information about supported gateways, see the "Voice Gateway Model Summary" section on page 39-9.

E1 CAS

Some Cisco gateways in H.323 mode can support the E1 CAS trunk interface that provides up to 32 connections on the link. You must configure the E1 CAS signaling interface on the gateway, not in Cisco Unified CallManager Administration. Both ends of the E1 link must specify E1 CAS signaling. For a list of H.323 gateways that support E1 CAS, see the "Voice Gateway Model Summary" section on page 39-9. Refer to documentation for the specific gateway for configuration information.

Related Topics

- Loop-Start Signaling, page 40-4
- Ground-Start Signaling, page 40-4
- E&M Signaling, page 40-4

Digital Telephony Protocols

Digital telephony protocols use common channel signaling (CCS), a dedicated channel that carries only signals. In a T1 link, one channel carries the signals while the other channels carry voice or data. The latest generation of CCS is known as Signaling System 7 (SS7) and provides supervision, addressing, tones, and a variety of services such as automatic number identification (ANI).

Integrated Services Digital Network (ISDN) is a set of international standards for user access to private or public network services. ISDN provides both circuit-based and packet-based communications to users.

Cisco CallManger can support these ISDN protocols:

- Basic Rate Interface (BRI), page 40-6
- T1 Primary Rate Interface (T1 PRI), page 40-6
- E1 Primary Rate Interface (E1 PRI), page 40-6
- Q.Signaling (QSIG), page 40-6

Basic Rate Interface (BRI)

Basic rate interface (BRI) , which is used for small office and home communications links, provides two B-channels for voice and data and one D-channel for signaling.

Related Topics

- T1 Primary Rate Interface (T1 PRI), page 40-6
- E1 Primary Rate Interface (E1 PRI), page 40-6
- Q.Signaling (QSIG), page 40-6

T1 Primary Rate Interface (T1 PRI)

T1 Primary rate interface (PRI) is used for corporate communications links in North America and Japan. T1 PRI provides 23 B-channels for voice and data and one D-channel for common channel signaling. T1 PRI uses a communication rate of 1.544Mbps.

Related Topics

- Basic Rate Interface (BRI), page 40-6
- E1 Primary Rate Interface (E1 PRI), page 40-6
- Q.Signaling (QSIG), page 40-6

E1 Primary Rate Interface (E1 PRI)

E1 PRI Primary rate interface (PRI) is used for corporate communications in Europe. E1 PRI provides 30 B-channels for voice and data , one D-channel for common signaling, and one framing channel. E1 PRI uses a rate of 2.048 Mbps.

Related Topics

- Basic Rate Interface (BRI), page 40-6
- T1 Primary Rate Interface (T1 PRI), page 40-6
- Q.Signaling (QSIG), page 40-6

Q.Signaling (QSIG)

Because enterprises maintain existing telecommunication equipment from a variety of vendors, the protocol system, Q signaling (QSIG), provides interoperability and feature transparency between a variety of telecommunications equipment.

The QSIG protocol, a series of international standards, defines services and signaling protocols for Private Integrated Services Networks (PISNs). These standards use Integrated Services Digital Networks (ISDN) concepts and conform to the framework of International Standards for Open Systems Interconnection as defined by ISO/IEC. The QSIG protocol acts as a variant of ISDN D-channel voice signaling. The ISDN Q.921 and Q.931 standards provides the basis for QSIG protocol, which sets worldwide standard for PBX interconnection.

The QSIG protocol enables Cisco voice switching services to connect to PBXs and key systems that communicate by using QSIG protocol. For QSIG basic call setup, Cisco devices can route incoming voice calls from a private integrated services network exchange (PINX) device across a WAN to a peer Cisco device that can transport the signaling and voice packets to another PINX device, which are PBXs, key systems, or Cisco Unified CallManager servers that support QSIG protocol.

In a basic QSIG call, a user in a PINX can place a call to a user that is in a remote PINX. The called party receives the caller name or number as the call rings. The calling party receives the called name and number when the user phone rings in the remote PINX. All the features that are available as a PBX user operate transparently across the network. QSIG protocol provides supplementary and additional network features, as defined for PISNs, if the corresponding set of QSIG features are supported by both ends of the call.

To make supplementary features available to network users, ensure that all PBXs in the network support the same feature set.

Cisco tested Cisco Unified CallManager QSIG feature functionality with the following PBX vendors: Lucent/Avaya Definity G3R using T1 or E1, Avaya MultiVantage and Communication Manager, Alcatel 4400 using E1 or T1, Ericsson MD110 using E1, Nortel Meridian using E1 or T1, Siemens Hicom 300 E CS using T1, Siemens Hicom 300 E using E1, and Siemens HiPath 4000.

Cisco Unified CallManager supports the following QSIG features:

- Annex M.1 (Message Tunneling for QSIG), page 40-7

Tip Annex M.1 provides support only for Cisco Unified CallManager clusters that use intercluster trunks. Cisco Unified CallManager does not support Annex M.1 with PBXs.

- Basic Call for QSIG, page 40-8
- Call Completion, page 40-8
- Call Diversion, page 40-9
- Call Transfer, page 40-10
- Compatibility with Older Versions of QSIG Protocol (ECMA), page 40-10
- Facility Selection and Reservation, page 40-11
- Identification Services, page 40-11
- Message Waiting Indication (MWI) Service, page 40-13
- Path Replacement, page 40-13

Annex M.1 (Message Tunneling for QSIG)

The Annex M.1 feature uses intercluster trunks and H.225 trunks to transport (tunnel) non-H.323 protocol information in H.323 signaling messages between Cisco Unified CallManagers. Annex M.1 supports QSIG calls and QSIG call independent signaling connections. After you complete intercluster trunk configuration in Cisco Unified CallManager Administration, QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, Message Waiting Indication, and Path Replacement.

Note For designated third-party switch equipment, the Annex M.1 feature can also use H.323 gateways to transport (tunnel) non-H.323 protocol information in H.323 signaling messages between Cisco Unified CallManagers. Refer to the Cisco Unified CallManager Compatibility Matrix for information about Annex M.1 feature interoperability with third-party vendors.

Tip If you use a gatekeeper, you must configure every gateway in the network for QSIG tunneling. If any gateway in the network does not support QSIG tunneling, calls drop at the intercluster trunk that is configured for QSIG tunneling.

For Cisco Unified CallManager to support QSIG tunneling, you must choose the QSIG option in the Tunneled Protocol drop-down list box and check the Path Replacement Support check box in the Trunk Configuration window in Cisco Unified CallManager Administration. By default, Cisco Unified CallManager sets the option in the Tunneled Protocol drop-down list box to None; after you configure the QSIG Tunneled Protocol option, the Path Replacement Support check box automatically becomes checked. If you do not require path replacement over Annex M.1 or QSIG-tunneled trunks, you can uncheck the check box.

When you set the Tunneled Protocol field to None, Cisco Unified CallManager automatically grays out the Path Replacement Support check box. When you set the Tunneled Protocol field to QSIG, you cannot configure the Redirecting Number IE Delivery (Inbound), Redirecting Number IE Delivery (Outbound), or Display IE Delivery options.

Tip Cisco Unified CallManager does not support protocol profile 0x91 ROSE encoding with Annex M.1.

Basic Call for QSIG

QSIG basic call setup provides the dynamic establishment of voice connections from an originating PINX (PBX or Cisco Unified CallManager) across a private network or virtual private network (VPN) to another PINX. You must use digital T1 or E1 primary rate interface (PRI) trunks to support QSIG protocol.

Call Completion

The following Call Completion services, which rely on the Facility Selection and Reservation feature, provide Cisco Call Back functionality over QSIG enabled trunks:

- Completion of Calls to Busy Subscribers (CCBS)—When a calling party receives a busy tone, the caller can request that the call complete when the busy destination hangs up the phone and becomes available.
- Completion of Calls on No Reply (CCNR)—When a calling party receives no answer at the destination, the calling party can request that the call complete after the activity occurs on the phone of the called party.

Cisco Unified CallManager and the Call Completion services use the CallBack softkey on supported Cisco Unified IP Phone models 7940, 7960, and 7970 in a Cisco Unified CallManager cluster or over QSIG trunks. Likewise, the following devices support QSIG Call Completion services:

- Cisco Unified IP Phone Models 7905, 7910, 7912, 7940, 7960, 7970
- Cisco VGC Phone, Cisco IP Communicator, and Cisco SCCP Phone
- CTI route point that forwards calls to supported devices

  The Callback Calling Search Space service parameter, which works with the Cisco Unified CallManager service, allows an originating PINX to route a call setup request to a CTI device that exists on the terminating PINX. This functionality supports CTI applications, such as Cisco Unified CallManager Attendant Console, Cisco Unified CallManager Assistant, and so on. For more information on this service parameter, click the **?** that displays in the upper corner of the Service Parameter window.
- QSIG trunks

In addition to configuring the Cisco Call Back feature in Cisco Unified CallManager Administration, as described in the "Cisco Call Back" section on page 4-1, you may need to update the default settings for the Cisco Call Back service parameters; that is, if the Cisco Technical Assistance Center (TAC) directs you to do so. Cisco Call Back service parameters include Connection Proposal Type, Connection Response Type, Callback Request Protection Timer, Callback Recall Timer, and Callback Calling Search Space. For information on these parameters, click the **?** that displays in the upper corner of the Service Parameter window.

For additional information on Cisco Call Back support, for example, how the feature works for QSIG-supported and Cisco Unified CallManager intracluster calls, refer to the "Cisco Call Back" section on page 4-1.

Call Diversion

Cisco Unified CallManager supports call diversion by rerouting and call diversion by forward switching. When call diversion by rerouting occurs, the originating PINX receives a request from the receiver of the call to divert the call to another user. The system creates a new call between the originator and the diverted-to user, and an additional CDR gets generated.

In Cisco Unified CallManager Administration, the Cisco CallManager service uses the following parameters to perform call diversion by rerouting: Call Diversion by Reroute Enabled and Call Reroute T1 Timer. If you want to use call diversion by rerouting, you must set the service parameters to the values that are specified in the **?** help, which displays when you click the **?** in the upper corner of the Service Parameter window. If you do not configure the service parameters, call diversion by forward switching automatically occurs.

Cisco Unified CallManager cannot request that the originating PINX divert the call, but Cisco Unified CallManager can validate the directory number to which the call is diverted by terminating restriction QSIG messages. Call diversion by rerouting does not support non-QSIG trunks. If you do not use a uniform dial plan for your network, use call diversion by forward switching and path replacement to optimize the path between the originating and terminating users.

If the receiver of the incoming call and the diverted-to user exist in the same PINX, Cisco Unified CallManager uses call diversion by forward switching. If call diversion by rerouting is not successful for any reason, for example, the rerouting timer expires, forward switching occurs.

QSIG diversion supplementary services provide call-forwarding capabilities that are similar to familiar Cisco Unified CallManager call-forwarding features, as indicated in the following list:

- Call Forward All (CFA) configuration supports Call Forwarding Unconditional (SS-CFU).
- Call Forward Busy (CFB) configuration supports Call Forwarding Busy (SS-CFB).
- Call Forward No Answer (CFNA) configuration supports Call Forwarding No Reply (SS-CFNR).
- Cisco Unified CallManager does not support Call Deflection (SS-CD).

To provide feature transparency with other PBXs in the network, the system passes information about a forwarded call during the call setup and connection over QSIG trunks. Phone displays can present calling name/number, original called name/number, and last redirecting name/number information to show the destination of the forwarded call.Call identification restrictions can impact what displays on the phone. See the "Identification Services" section on page 40-11 for more information.

QSIG supplementary services can provide the information to place the voice message from a diverted call into the originally called party voice mailbox. Be aware that voice-mail configuration may override call-forwarding configuration settings.

Cisco Unified CallManager does not invoke call diversion by rerouting when the system forwards the call to the voice mailbox. If the connection to the voice mail server occurs over a Q.SIG trunk and you want to use call diversion by rerouting, you must enter the voice mail pilot number in the appropriate Coverage/Destination field instead of checking the Voice Mail check box in the Directory Number Configuration window.

Tip When calls are forwarded among multiple PINXs, a forwarding loop can result. To avoid calls being caught in a looping condition, or entering a long forwarding chain, configure the Forward Maximum Hop Count service parameter for the Cisco CallManager service. Setting this service parameter above 15 makes your QSIG configuration noncompliant with international standards.

Call Transfer

Cisco Unified CallManager supports call transfer by join only.

When a user transfers a call to another user, the QSIG identification service changes the connected name and number that displays on the transferred party phone. Call identification restrictions can impact what displays on the phone.

The call transfer supplementary service interacts with the path replacement feature to optimize the trunk connections when a call transfers to a caller in another PINX. For more information about path replacement, see the "Path Replacement" section on page 40-13.

Compatibility with Older Versions of QSIG Protocol (ECMA)

To create CallManager compatibility with your version of the QSIG protocol, configure the ASN.1 Rose OID Encoding and QSIG Variant service parameters.

Tip For more information on these parameters, click the **?** that displays in the upper corner of the Service Parameter window.

If you choose ECMA for the QSIG Variant parameter, you must choose the Use Global Value (ECMA) setting for the ASN.1 Rose OID Encoding service parameter. If you choose ISO for the QSIG Variant parameter, you normally choose the Use Local Value setting for the ASN.1 Rose OID Encoding service parameter. Other configurations may be needed in unusual situations.

If you configure the QSIG Variant service parameter, a warning message indicates that Cisco Unified CallManager does not support ECMA with QSIG tunneling over intercluster trunks (Annex M.1). To use ECMA, verify that the None option displays for the Tunneled Protocol drop-down list box in the Trunk Configuration window.

Cisco Unified CallManager supports using Annex M.1 to tunnel QSIG over intercluster trunks. To configure Annex M.1, set the ASN.1 Rose OID Encoding to Use Global Valueless) and the QSIG Variant to ISO (Protocol Profile 0x9F).

Facility Selection and Reservation

The facility selection and reservation feature allows you to make calls by using mixed route lists, which contain route groups that use different protocols. This feature supports mixed route lists that include the following types of facilities:

- E1 or T1 PRI trunks that use the QSIG protocol
- E1 or T1 PRI trunks that use a protocol other than QSIG
- T1-CAS gateways
- FXO ports
- Intercluster trunks

Tip You cannot add route groups with H.323 gateways to a route list that includes QSIG route groups.

When you configure the route list, configure the QSIG route groups as the first choice, followed by the non-QSIG route groups that serve as alternate connections to the PSTN. Make sure that you include additional route groups for QSIG calls in addition to the private network QSIG facilities. When no QSIG trunks are available for a call, you want to provide alternate routes over the PSTN for calls.

If a call requires a QSIG facility, Cisco Unified CallManager hunts through the route groups to reserve the first available QSIG facility. If a QSIG facility is unavailable, Cisco Unified CallManager uses a non-QSIG facility to failover to the PSTN.

If a call does not require a QSIG facility, Cisco Unified CallManager hunts through the route groups to find the first available facility.

The Path Replacement, Message Waiting Indication, and Call Completion supplementary services require a QSIG facility to meet QSIG signaling compliance requirements. If a QSIG facility is not available for one of the aforementioned services, the call does not meet QSIG signaling compliance requirements, and the feature fails.

Identification Services

When a call alerts and connects to a PINX, identification services can display the caller name/ID on a phone in the terminating PINX, and, likewise, the connected party name/ID on a phone in the originating PINX. QSIG identification restrictions allow you to control the presentation or display of this information between Cisco Unified CallManager and the connected PINX.

Supported supplementary services apply on a per-call basis, and presentation settings for call identification information are set at both ends of the call. Cisco Unified CallManager provides configuration settings to control the following caller identification number (CLID) and caller name (CNAM) information on phone displays:

- Calling Line Identification Presentation/Restriction—Displays the calling number (CLIP) or restricts the display of the calling number (CLIR).
- Calling Name Identification Presentation/Restriction—Displays the calling name (CNIP) or restricts the display of the calling name (CNIR).
- Connected Line Identification Presentation/Restriction—Displays the number of the connected line (COLP) or restricts the display of the connected line (COLR).
- Connected Name Identification Presentation/Restriction—Displays the name of the connected party (CONP) or restricts the display of the connected name (CONR).

Configuration settings for the outgoing call get sent to the terminating PINX, where the settings may get overwritten. The connected line and name configuration gets set on the terminating side of the call; after the originating PINX receives the configuration settings, the originating PINX may override the configuration.

Tip When you restrict a name, the display shows "Private," and the display remains blank for a restricted calling line number.

You can allow or restrict display information for all calls by configuring fields in the Gateway Configuration window. Or, you can control display information on a call-by-call basis by using fields in the Route Patterns and Translation Patterns windows. The presentation setting for the gateway overrides the setting for the route pattern. Translation pattern presentation settings override route pattern presentation settings.

Cisco Unified CallManager supports "Alerting on ring" only, and the QSIG Alerting Name that you configure allows you to send and receive call name information while the phone rings. In the Directory Number Configuration window in Cisco Unified CallManager Administration, you configure the Alerting Name field for shared and nonshared directory numbers. When two phones ring for the shared directory number, the name that you entered in the Alerting Name field displays on the phone of the called party at the terminating PINX, unless translation pattern restrictions affect the information that displays. Route pattern restrictions may affect the information that displays on caller phone at the originating PINX.

Tip You configure Alerting Name identification restrictions by setting the Connected Name configuration parameters.

If you do not configure an Alerting Name, only the directory number displays on the calling party phone when alerting occurs. If you configure a Display Name configured for the called party, the Display Name displays on the calling party phone when the call connects. If you do not enter a Display Name or an Alerting Name, no name displays on the calling party phone during the call. You cannot use Alerting Name with the following device types:

- PRI trunks
- FXS/FXO ports for MGCP gateways
- MGCP T1-CAS gateways

Message Waiting Indication (MWI) Service

In a QSIG network, when a PINX has a connected voice-messaging system that services users in another PINX, the message center PINX can send the following message waiting indication (MWI) signals to the other PINX:

- MWI Activate—Send a signal to another PINX to activate MWI on the served user's phone after the voice-messaging system receives a message for that phone.
- MWI De-activate—Send a signal to deactivate the MWI after the user listens to messages in the associated voice-messaging system.

Note Cisco Unified CallManager does not support the MWI interrogation service.

A PINX that is not a message center can receive MWI signals and perform the following tasks:

- MWI Activate—Receive a signal from another PINX to activate MWI on the served user's phone.
- MWI De-activate—Receive a signal to deactivate the MWI on the served user phone.

If the voice-messaging system connects to Cisco Unified CallManager by using QSIG connections or by using the Cisco Messaging Interface (CMI), the message waiting indicators get set based on QSIG directives.

When a call is forwarded to a number and then diverted to a voice-messaging system, QSIG supplementary services can provide the information to place the voice message in the originally called party voice mailbox.

The Message Waiting Indication service, which uses the existing dial number for message waiting that is set up in Cisco Unified CallManager Administration, does not require any additional configuration.

Path Replacement

In a QSIG network, after a call is transferred or forwarded to a phone in a third PINX, multiple connections through several PINX(s) can exist for the call. After the call connects, the path replacement feature drops the connection to the transit PINX(s) and creates a new call connection to the terminating PINX.

Note Cisco Unified CallManager provides “requesting” and “cooperating” PINX messages only. If configured for QSIG, Cisco Unified CallManager responds to third-party vendor PINX “inviting” messages, although Cisco Unified CallManager will not originate “inviting” messages.

Cisco Unified CallManager does not support path retention.

Cisco Unified CallManager initiates path replacement for calls that are transferred by joining and for calls that are diverted by forward switching only. Calls that involve multiple trunks, for example, conference calls, do not use path replacement; however, if you choose the QSIG option for the Tunneled Protocol drop-down list box and check the Path Replacement Support check box for gatekeeper-controlled or non-gatekeeper-controlled intercluster trunks, path replacement occurs over the intercluster trunk and the other QSIG intercluster or PRI trunk that is used to transfer or divert the call.

When you use CTI applications with path replacement, the leg of the call that uses path replacement has a different Global Caller ID than the originating leg of the call. After a call is forwarded or transferred, if the remaining parties use the same Cisco Unified CallManager, two Global Caller IDs exist, one for each party. The system deletes one of the Global Caller IDs, both parties in the call have the same Global Caller ID.

Tip This section provides information on a few path replacement service parameters. For a complete list of service parameters and for detailed information on the parameters, click the **?** that displays in the upper corner of the Service Parameter Configuration window.

Because the QSIG protocol passes the extension number or directory number but does not pass translated or inserted numbers, use QSIG features, such as path replacement, in a network with a uniform dial plan. When a private network uses nonunique directory numbers in the dial plan, you must reroute calls through a PINX ID, which is a unique directory number for every PINX in the network. The path replacement feature uses the PINX ID, if configured, instead of the called or calling party number that the "Identification Services" section on page 40-11 describes. To configure the PINX ID, perform the following tasks in Cisco Unified CallManager Administration:

- Configure the PINX ID service parameter(s) for the Path Replacement feature. (The Path Replacement feature uses the Cisco CallManager service.)
- Create a call pickup group that includes only the PINX ID.

Tip Reserve the PINX ID call pickup group for PINX ID usage. Do not add other directory numbers to this call pickup group.

Cisco Unified CallManager provides the Path Replacement Calling Search Space service parameter, so you can configure the calling search space that the cooperating PINX uses to send the outbound SETUP message to the requesting PINX. If you do not specify a value for the Path Replacement Calling Search Space service parameter, the requesting PINX uses the calling search space of the end user that is involved in the call.

You configure Path Replacement settings in the Service Parameter window for the Cisco CallManager service. Path Replacement service parameters include Path Replacement Enabled, Path Replacement on Tromboned Trunks, Start Path Replacement Minimum Delay Time, Start Path Replacement Maximum Delay Time, Path Replacement PINX ID, Path Replacement Timers, Path Replacement Calling Search Space, and so on. To obtain information about these parameters, click the **?** that displays in the Service Parameter window.

Path replacement performance counters allow you to track when path replacement occurs. For information on performance counters, refer to the *Cisco Unified CallManager Serviceability System Guide*.

For each call, the system generates more than one CDR for the path replacement feature. One CDR gets generated for the caller at the originating PINX; another CDR gets generated for the called party at the PINX where path replacement is initiated.

Note When a Cisco SoftPhone user chooses to perform a consultive transfer to move a call to another PINX, path replacement can occur; if the user performs a direct (blind) transfer, path replacement cannot occur. For more information about Cisco SoftPhone, refer to the Cisco SoftPhone documentation that supports your version of the application.

QSIG Interface to Cisco Unified CallManager

For Cisco Unified CallManager to support QSIG functionality, QSIG must be back-hauled directly to Cisco Unified CallManager. Cisco Unified CallManager interconnects to a QSIG network by using an MGCP gateway and T1 or E1 PRI connections to the PISN. The MGCP gateway establishes the call connections. By using the PRI backhaul mechanism, the gateway passes the QSIG messages to Cisco Unified CallManager to enable setting up QSIG calls and sending QSIG messages to control features.

When a PBX is connected to a gateway that is using QSIG via H.323, calls that are made between phones on the PBX and IP phones that are attached to the Cisco Unified CallManager can have only basic PRI functionality. The gateway that terminates the QSIG protocol provides only the Calling Line Identification (CLID) and Direct Inward Dialed (DID) number rather than Cisco Unified CallManager providing the information.

Related Topics

- Basic Rate Interface (BRI), page 40-6
- E1 Primary Rate Interface (E1 PRI), page 40-6
- T1 Primary Rate Interface (T1 PRI), page 40-6

Where to Find More Information

Related Topics

- Understanding Session Initiation Protocol (SIP), page 41-1
- Gateway Configuration, page 69-1
- Gatekeeper Configuration, page 68-1
- Understanding Cisco Unified CallManager Voice Gateways, page 39-1
- Gateway Configuration Checklist, page 39-16
- Trunk Configuration Checklist, page 42-6
- Trunk Configuration, page 71-1

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design*
- *Configuring Cisco Unified Communications Voice Gateways*

CHAPTER 41

Understanding Session Initiation Protocol (SIP)

Understanding Session Initiation Protocol (SIP) describes SIP and the interaction between SIP and Cisco Unified CallManager.

This section covers the following topics:

- SIP Networks, page 41-1
- SIP and Cisco Unified CallManager, page 41-2
- SIP Functions That Are Supported in Cisco Unified CallManager, page 41-5
- SIP Trunk Configuration Checklist, page 41-13
- Cisco Unified CallManager SIP Endpoints Overview, page 41-13
- SIP Line Side Overview, page 41-15
- SIP Standards, page 41-15
- Cisco Unified CallManager Functionality Supported by SIP Phones, page 41-18
- Where to Find More Information, page 41-20

SIP Networks

A SIP network uses the following components:

- SIP Proxy Server—The proxy server works as an intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
- Redirect Server—The redirect server provides the client with information about the next hop or hops that a message should take, and the client then contacts the next hop server or user agent server directly.
- Registrar Server—The registrar server processes requests from user agent clients for registration of their current location. Redirect or proxy servers often contain registrar servers.
- User Agent (UA)— UA comprises a combination of user agent client (UAC) and user agent server (UAS) that initiates and receives calls. A UAC initiates a SIP request. A UAS, a server application, contacts the user when it receives a SIP request. The UAS then responds on behalf of the user. Cisco Unified CallManager can act as both a server and a client (a back-to-back user agent).

SIP uses a request/response method to establish communications between various components in the network and to ultimately establish a call or session between two or more endpoints. A single session may involve several clients and servers.

Identification of users in a SIP network works through

- A unique phone or extension number.
- A unique SIP address that appears similar to an e-mail address and uses the format `sip:<userID>@<domain>`. The user ID can be either a user name or an E.164 address. Cisco Unified CallManager only supports E.164 addresses; it does not support email addresses.
- An email address format (employee@company.com) that is supported on Cisco Unified CallManager with SIP route patterns.

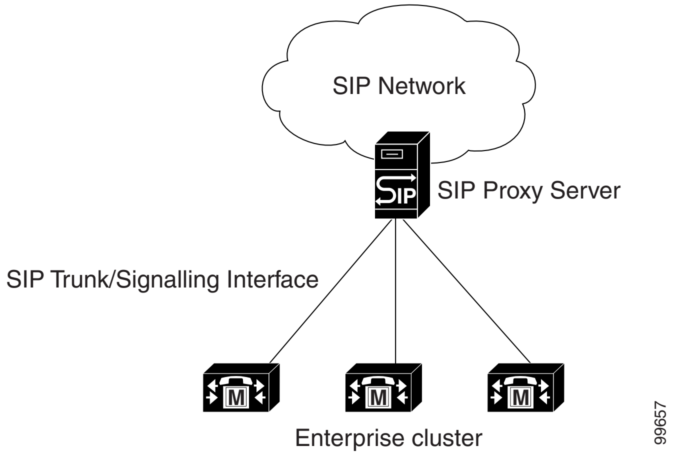
SIP and Cisco Unified CallManager

All protocols require that either a signaling interface (trunk) or a gateway be created to accept and originate calls. For SIP, the user must configure a SIP trunk. For more information, refer to Trunk Configuration in the *Cisco Unified CallManager Administration Guide*.

SIP trunks connect Cisco Unified CallManager networks and SIP networks that are served by a SIP proxy server. As with other protocols, SIP components fit under the device layer of Cisco Unified CallManager architecture. As is true for the H.323 protocol, multiple logical SIP trunks can be configured in the Cisco Unified CallManager database and associated with route groups, route lists, and route patterns. To provide redundancy, in the event of failure of one logical SIP interface, other logical SIP interfaces provide services in the same route group list. Assigning multiple Cisco Unified CallManager nodes under SIP trunk device pools also achieves redundancy.

SIP trunks support multiple port-based routing. Multiple SIP trunks on Cisco Unified CallManager can use port 5060, the default, which is configurable from the SIP Trunk Security Profile Configuration window. For TCP/UDP, SIP trunks use the remote host and local listening port to do the routing (the remote host can be IP, FQDN, or SRV). For TLS, SIP trunks use X.509 Subject Name to do the routing. For SIP trunks, Cisco Unified CallManager only accepts calls from the SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk.

Figure 41-1 SIP and Cisco Unified CallManager Interaction



Media Termination Point (MTP) Devices

You can configure Cisco Unified CallManager SIP devices (lines and trunks) to always use an MTP. If the configuration parameters are set to not use an MTP (default case), Cisco Unified CallManager will attempt to dynamically allocate an MTP if the DTMF methods for the call are not compatible. For example, SCCP phones support only out-of-band DTMF, and Cisco SIP phones (model 7905, 7912, 7940, 7960) support RFC2833. Because the DTMF methods are not identical, Cisco Unified CallManager will dynamically allocate an MTP. If, however, a SCCP phone that supports RFC2833 and out-of-band, such as Cisco Unified IP Phone 7971, calls a Cisco SIP IP phone 7940, Cisco Unified CallManager will not allocate an MTP because both phones support RFC2833. By having the same type of DTMF method supported on each phone, no need for an MTP exists.

SIP Service Parameters

You can individually configure SIP timers and counters for functionality on different servers. Refer to Service Parameters Configuration in the *Cisco Unified CallManager Administration Guide* for full information on how to configure service parameters.

SIP Timers and Counters

SIP timers and counters act as configurable service parameters. The following tables describe the various SIP timers and counters and give their default values and range values:

Table 41-1 SIP Timers That Are Supported in Cisco Unified CallManager

Timer	Default Value	Default Range	Definition
Trying	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait for a 100 response before retransmitting the INVITE.
Connect	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait for an ACK before retransmitting the 2xx response to the INVITE.
Disconnect	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait for a 2xx response before retransmitting the BYE request.
Expires	180000 milliseconds	60000 to 300000	Valid time that is allowed for an INVITE request.
rel1xx	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait before retransmitting the reliable1xx responses.
PRACK	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait before retransmitting the PRACK request.

Note When using TCP transport and a timer times out, the SIP device does not retransmit. The device relies on TCP to retry.

Table 41-2 SIP Retry Counters That Are Supported in Cisco Unified CallManager

Retry Counter	Default Value	Default Range	Definition
INVITE	6	1 to 10	Number of INVITE retries
Response	6	1 to 10	Number of RESPONSE retries
BYE	10	1 to 10	Number of BYE retries
Cancel	10	1 to 10	Number of Cancel retries
PRACK	6	1 to 10	Number of PRACK retries
Rel1xx	10	1 to 10	Number of Reliable 1xx response retries

Supported Audio Media Types

The following table describes the various supported audio media types:

Table 41-3 Supported Audio Media Types

Type	Encoding Name	Payload Type	Comments
G.711 u-law	PCMU	0	
GSM Full-rate	GSM	3	
G.723.1	G723	4	
G.711 A-law	PCMA	8	
G.722	G722	9	
G.728	G728	15	
G.729	G729	18	Support all combinations of annex A and B
RFC2833 DTMF	Telephony-event	Dynamically Assigned	Acceptable range is 96 - 127

Supported Video Media Types

The following table describes the various supported video media types:

Table 41-4 Supported Video Media Types

Type	Encoding Name	Payload Type
H.261	H261	31
H.263	H263	34
H.263+	H263-1998	Acceptable range is 96 - 127

Table 41-4 Supported Video Media Types (continued)

Type	Encoding Name	Payload Type
H.263++	H263-2000	Acceptable range is 96 - 127
H.264	H264	Acceptable range is 96 - 127

Supported Application Media Type

The following table describes the supported application media types:

Table 41-5 Supported Application Media Types

Type	Encoding Name	Payload Type
H.224 FECC	H224	Acceptable range is 96 - 127

Supported T38fax Payload Type

The following table describes the various supported application media types:

Table 41-6 Supported T38fax Payload type

Type	Encoding Name	Payload Type
T38fax	Not applied	Not applicable

SIP Profiles for Trunks

SIP trunks and SIP endpoints use SIP profiles. SIP trunks use SIP profiles to define the Default Telephony Event Payload Type and the Disable Early media on 180. For more information on SIP profiles, see the "SIP Profiles for Endpoints" section on page 41-19 and SIP Profile Configuration in the *Cisco Unified CallManager Administration Guide*.

SIP Functions That Are Supported in Cisco Unified CallManager

Cisco Unified CallManager supports the following functions and features for SIP calls:

- Basic Calls Between SIP Endpoints and Cisco Unified CallManager, page 41-6
- DTMF Relay Calls Between SIP Endpoints and Cisco Unified CallManager, page 41-6
- Supplementary Services That Are Initiated If an MTP Is Allocated, page 41-8
- Ringback Tone During Blind Transfer, page 41-8
- Supplementary Services That Are Initiated by SIP Endpoint, page 41-9
- Enhanced Call Identification Services, page 41-9
- Redirecting Dial Number Identification Service (RDNIS), page 41-12
- Redirection, page 41-12

Basic Calls Between SIP Endpoints and Cisco Unified CallManager

This section includes three basic calling scenarios. Two scenarios describe incoming and outgoing calls, while the other one describes the use of early media which is a media connection prior to the connection or answer of a call.

- Basic Outgoing Call, page 41-6
- Basic Incoming Call, page 41-6
- Use of Early Media, page 41-6

Basic Outgoing Call

You can initiate outgoing calls to a SIP device from any Cisco Unified CallManager device. A Cisco Unified CallManager device includes SCCP or SIP IP phones or fax devices that are connected to Foreign Exchange Station (FXS) gateways. For example, an SCCP IP phone can place a call to a SIP endpoint. The SIP device answering the call triggers media establishment.

Basic Incoming Call

Any device on the SIP network, including SIP IP Phones or fax devices that are connected to FXS gateways can initiate incoming calls. For example, a SIP endpoint can initiate a call to an SCCP IP Phone. The SCCP IP phone that answers the call triggers media establishment.

Use of Early Media

While the PSTN provides inband progress information to signal early media (such as a ring tone or a busy signal), the same does not occur for SIP. The originating party includes Session Description Protocol (SDP) information, such as codec usage, IP address, and port number, in the outgoing INVITE message. In response, the terminating party sends its codec, IP address, and port number in a 183 Session Progress message to indicate possible early media.

The 183 Session Progress response indicates that the message body contains information about the media session. Both 180 Alerting and 183 Session Progress messages may contain SDP, which allows an early media session to be established prior to the call being answered.

When early media needs to be delivered to SIP endpoints prior to connection, Cisco Unified CallManager always sends a 183 Session Progress message with SDP. Although Cisco Unified CallManager does not generate a 180 Alerting message with SDP, it does support the 180 Alerting message with SDP when it receives one.

The SIP Profile Configuration window contains a Disable Early Media on 180 check box. Check the check box to play local ringback on the called phone and connect the media upon receipt of the 200OK response. See the "SIP Profile Configuration Settings" section on page 79-2.

DTMF Relay Calls Between SIP Endpoints and Cisco Unified CallManager

MTPs are now dynamically allocated, if needed, based on the DTMF methods used on each endpoint.

Forwarding DTMF Digits from SIP Devices to Gateways or Interactive Voice Response (IVR) Systems for Dissimilar DTMF methods

The following example (Figure 41-2) shows the MTP software device processing inband DTMF digits from the SIP phone to communicate with the Primary Rate Interface (PRI) gateway. The RTP stream carries RFC 2833 DTMF, as indicated by a dynamic payload type.

Figure 41-2 Forwarding DTMF Digits

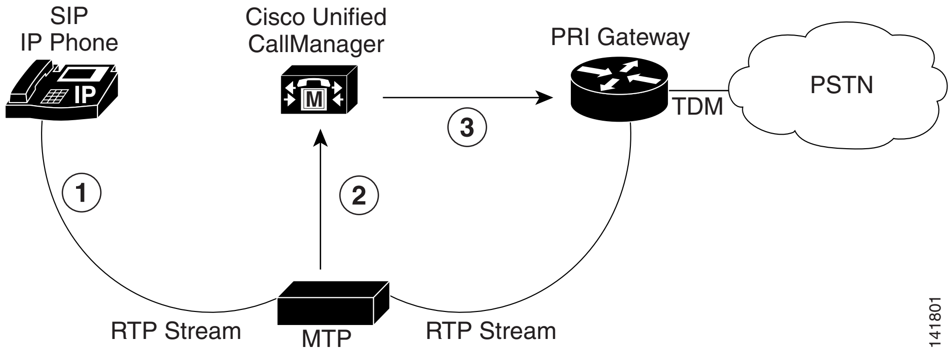


Figure 41-2 begins with media streaming, and the MTP device has been informed of the DTMF dynamic payload type:

1. The SIP phone initiates a payload type response when the user enters a number on the keypad. The SIP phone transfers the DTMF in-band digit (per RFC 2833) to the MTP device.
2. The MTP device extracts the in-band DTMF digit and passes the digit out of band to Cisco Unified CallManager.
3. Cisco Unified CallManager then relays the DTMF digit out of band to the gateway or IVR system.

Generating DTMF Digits for Dissimilar DTMF Methods

As discussed in DTMF Relay Calls Between SIP Endpoints and Cisco Unified CallManager, page 41-6, SIP sends DTMF in-band digits, while Cisco Unified CallManager only supports out-of-band digits. The software MTP device receives the DTMF out-of-band tones and generates DTMF in-band tones to the SIP client.

Figure 41-3 Generating DTMF Digits

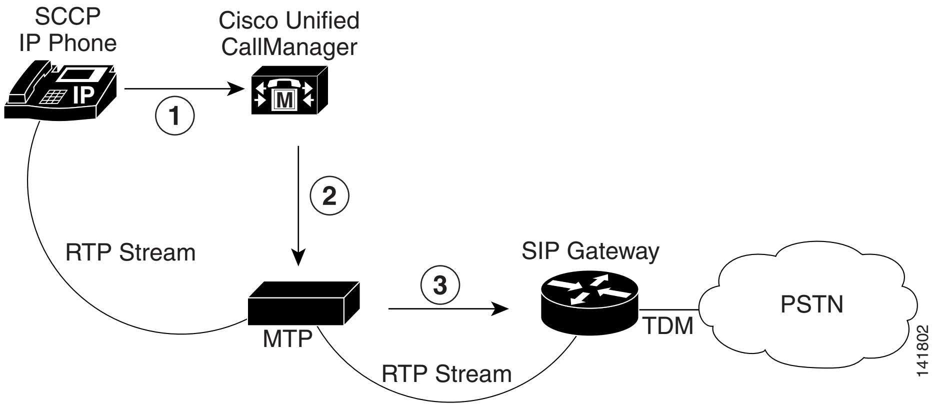


Figure 41-3 begins with media streaming, and the MTP device has been informed of the dynamic DTMF payload type.

1. The SCCP IP phone user presses buttons on the keypad. Cisco Unified CallManager collects the out-of-band digits from the SCCP IP phone.
2. Cisco Unified CallManager passes the out-of-band digits to the MTP device.
3. The MTP device converts the digits to RFC 2833 RTP compliant in-band digits and forwards them to the SIP client.

Supplementary Services That Are Initiated If an MTP Is Allocated

The system supports all supplementary services that the SCCP endpoint initiates during a SIP call. Cisco Unified CallManager internally manages SCCP endpoints without affecting the connecting SIP device. Any changes to the original connecting information get updated with re-INVITE or UPDATE messages that use the Remote-Party-ID header. See *SIP Extensions for Caller Identity and Privacy* for more information on the Remote-Party-ID header.

The section, Ringback Tone During Blind Transfer, page 41-8, describes a blind transfer, which is unique as a supplementary service because it requires Cisco Unified CallManager to provide a media announcement.

Ringback Tone During Blind Transfer

For SCCP initiated blind transfers, Cisco Unified CallManager needs to generate tones or ringback after a call has already connected. In other words, Cisco Unified CallManager provides a media announcement for blind transfers.

A blind transfer works when the transferring phone connects the caller to a destination line before the target of the transfer answers the call. A blind transfer differs from a consultative, or attended transfer, in which one transferring party either connects the caller to a ringing phone (ringback received) or speaks with the third party before connecting the caller to the third party

Blind transfers that are initiated from an SCCP IP phone allow ringback to the original, connected SIP device user. To accomplish ringback, Cisco Unified CallManager uses an annunciator software device that is often located with an MTP device.

With an annunciator, Cisco Unified CallManager can play predefined tones and announcements to SCCP IP phones, gateways, and other IP telephony devices. These predefined tones and announcements provide users with specific information on the status of the call.

Supplementary Services That Are Initiated by SIP Endpoint

The following sections describe supplementary services that a SIP endpoint can initiate.

- SIP–Initiated Call Transfer, page 41-9
- Call Hold, page 41-9
- Call Forward, page 41-9

SIP–Initiated Call Transfer

Cisco Unified CallManager does support SIP-initiated call transfer and does accept REFER requests or INVITE messages that include a Replaces header.

Call Hold

Cisco Unified CallManager supports call hold and retrieve that a SIP device initiates or that a Cisco Unified CallManager device initiates. For example, when a SCCP IP phone user retrieves a call another user placed on hold, Cisco Unified CallManager sends a re-INVITE message to the SIP proxy. The re-INVITE message contains updated Remote-Party-ID information to reflect the current connected party. If Cisco Unified CallManager originally initiated the call, the Party field in the Remote-Party-ID header gets set to calling; otherwise, it gets set to called. For more information on the Party field parameter, see Enhanced Call Identification Services, page 41-9.

Call Forward

Cisco Unified CallManager supports call forward that a SIP device initiates or that a Cisco Unified CallManager device initiates. With call forwarding redirection requests from SIP devices, Cisco Unified CallManager processes the requests. For call forwarding that is initiated by Cisco Unified CallManager, the system uses no SIP redirection messages. Cisco Unified CallManager handles redirection internally and then conveys the connected party information to the originating SIP endpoint through the Remote-Party-ID header.

Enhanced Call Identification Services

This section describes the following SIP identification services in Cisco Unified CallManager and how Cisco Unified CallManager conveys these identification services in the SIP:

- Line Identification Services
  - Calling Line Presentation (CLIP) and Restriction (CLIR)
  - Connected Line Presentation (COLP) and Restriction (COLR)
- Name Identification Services
  - Calling Name Presentation (CNIP) and Restriction (CNIR)
  - Connected Name Presentation (CONP) and Restriction (CONR)

Cisco Unified CallManager provides flexible configuration options to provide these identification services either on a call-by-call, or a statically preconfigured for each SIP signaling interface, basis.

Calling Line and Name Identification Presentation

Cisco Unified CallManager includes the calling line (or number) and name presentation information in the From and Remote-Party-ID headers of the initial INVITE message from Cisco Unified CallManager. The From header field indicates the initiator of the request. Cisco Unified CallManager uses Remote-Party-ID headers in 18x, 200 and re-INVITE messages to convey connected name and identification information. The Remote-Party-ID header also gives detailed descriptions of caller identity and privacy. Cisco Unified CallManager sets the Party field of the Remote-Party-ID header to calling for calling ID services.

Note See the *Cisco IOS SIP Configuration Guide* for more general information on Remote-Party-ID header.

Example

Bob Jones (with external phone number=8005550100) dials out to a SIP signaling interface; the From and Remote-Party-ID headers contain

```
From: “Bob Jones” <sip:8005550100@localhost>
Remote-Party-ID: “Bob Jones”<8005550100@localhost; user=phone>;
party=calling;screen=no;privacy=off
```

Calling Line and Name Identification Restriction

Calling line (or number) and name restrictions configuration occurs on the SIP signaling interface level or on a call-by-call basis. The SIP trunk level configuration takes precedence over the call-by-call configuration. To configure on a call-by-call basis, refer to the Route Group Configuration in the *Cisco Unified CallManager Administration Guide.*

Calling line and name restrictions configuration also occurs independently of each other. For example, you may choose to restrict only numbers and allow names to be presented.

Example 1

With a restricted calling name, Cisco Unified CallManager sets the calling name in the From header to a configurable string. Cisco Unified CallManager sets the display field in the Remote-Party-ID header to include the actual name but sets the Privacy field to name:

```
From: “Anonymous” <sip:8005550100@localhost>
Remote-Party-ID: “Bob Jones”<sip:9728135001@localhost;user=phone>;
party=calling;screen=no;privacy=name
```

Example 2

With a restricted calling number, Cisco Unified CallManager leaves out the calling line in the From header; however, Cisco Unified CallManager still includes the calling line in the Remote-Party-ID header but sets the Privacy field to privacy=uri:

```
From: “Bob Jones” <sip:@localhost>
Remote-Party-ID: “Bob Jones”<sip:8005550100@localhost;user=phone>;
party=calling;screen=no;privacy=uri
```

Example 3

With a restricted calling name and number, Cisco Unified CallManager sets the Privacy field to privacy=full in the Remote-Party-ID header:

```
From: “Anonymous” <sip:localhost>
Remote-Party-ID: “Bob Jones”<sip:8005550100@localhost;user=phone>;
party=calling;screen=no;privacy=full
```

Connected Line and Name Identification Presentation

Cisco Unified CallManager uses connected line and name identification as a supplementary service to provide the calling party with the connected party’s number and name. The From header field indicates the initiator of the request. Cisco Unified CallManager uses Remote-Party-ID headers in 18x, 200 and re-INVITE messages to convey connected information. Cisco Unified CallManager sets the Party field of Remote-Party-ID header to called.

Example 1

Cisco Unified CallManager receives an INVITE message with a destination address of 800555. Cisco Unified CallManager includes the connected party name in 18x and 200 messages as follows:

```
Remote-Party-ID: “Bob Jones”<98005550100@localhost; user=phone>;
party=called;screen=no;privacy=off
```

Connected Line and Name Identification Restriction

You can configure connected line (or number) and name restrictions on the SIP trunk level or on a call-by-call basis. The SIP trunk level configuration takes precedence over the call-by-call configuration. To configure on a call-by-call basis, refer to the Route Group Configuration in the *Cisco Unified CallManager Administration Guide*.

Similar to Calling ID services, users can restrict connected number and name independently of each other.

Example 1

Cisco Unified CallManager sets the display field in the Remote-Party-ID header to include the actual name, but sets the Privacy field to privacy=name:

```
Remote-Party-ID: “Bob Jones”<8005550100@localhost; user=phone>;
party=called;screen=no;privacy=name
```

Example 2

With a restricted connected number, Cisco Unified CallManager still includes the connected number in the Remote-Party-ID header but sets the Privacy field to privacy=uri:

```
Remote-Party-ID: “Bob Jones”<8005550100@localhost; user=phone>;
party=called;screen=no;privacy=uri
```

Example 3

With a restricted connected name and number, Cisco Unified CallManager sets the Privacy field to privacy=full in the Remote-Party-ID header:

```
Remote-Party-ID: “Bob Jones”<8005550100@localhost; user=phone>;
party=called;screen=no;privacy=full
```

Redirecting Dial Number Identification Service (RDNIS)

Cisco Unified CallManager uses the SIP Diversion header in the initial INVITE message to carry available RDNIS information.

Redirection

Previously, the redirection from the SIP network got handled at the SIP stack level, and the system accepted and forwarded all redirection requests to the contacts in the redirection response out to the same trunk on which the redirection response was received. No consulting or applying of any additional logic to handle or restrict how the call is redirected occurred. For example, if the redirection contact in a 3xx response to an outgoing INVITE was a Cisco Unified CallManager registered phone and the stack is handling redirection, the call gets redirected back out over the same trunk instead of being routed directly to the Cisco Unified CallManager phone. Getting redirected to a restricted phone number (such as an international number) means that handling redirection at the stack level will cause the call to be routed instead of being blocked. This represents the behavior you will get if the Redirect by Application check box on the SIP Profile Configuration window is unchecked.

Checking the Redirect by Application check box that is on the SIP Profile Configuration window and configuring this option on the SIP trunk allows the Cisco Unified CallManager administrator to

- Apply a specific calling search space to redirected contacts that are received in the 3xx response.
- Apply digit analysis to the redirected contacts to make sure that the call gets routed correctly.
- Prevent DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set.
- Allow other features to be invoked while the redirection is taking place.

For more information, see the "SIP Profile Configuration Settings" section on page 79-2 and Trunk Configuration in the *Cisco Unified CallManager Administration Guide*.

SIP Trunk Configuration Checklist

Table 41-7 provides an overview of the steps that are required to configure SIP trunk in Cisco Unified CallManager, along with references to related procedures and topics.

Table 41-7 Trunk Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Create a SIP profile (optional). Create a SIP trunk security profile (optional) Create a SIP trunk. Configure the destination address. Configure the destination port.	Configuring SIP Profiles, *Cisco Unified CallManager Administration Guide* Configuring a Trunk, *Cisco Unified CallManager Administration Guide* Trunk Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 2	Associate the SIP trunk to a Route Pattern or Route Group.	SIP Route Pattern Configuration, *Cisco Unified CallManager Administration Guide* Route Group Configuration, *Cisco Unified CallManager Administration Guide* Route List Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Configure SIP timers, counters, and service parameters, if necessary.	Service Parameters Configuration, *Cisco Unified CallManager Administration Guide.* For specific configurable values, see SIP Timers and Counters, page 41-3.
Step 4	Reset the SIP trunk	Configuring a Trunk, *Cisco Unified CallManager Administration Guide*

Cisco Unified CallManager SIP Endpoints Overview

The Cisco SIP IP phones 7911, 7941, 7961, 7970, and 7971 are deployed as a SIP endpoint in a Cisco Unified CallManager Back to Back User Agent (B2BUA) environment. The primary interface between the phone and other network components is the SIP protocol. In addition to SIP, other protocols are used for various functions such as DHCP for IP address assignment, DNS for domain name to address resolution, and TFTP for downloading image and configuration data.

This section provides an example illustration and brief description of the B2BUA and peer-to-peer environments.

Figure 41-4 Cisco Unified CallManager B2BUA Network

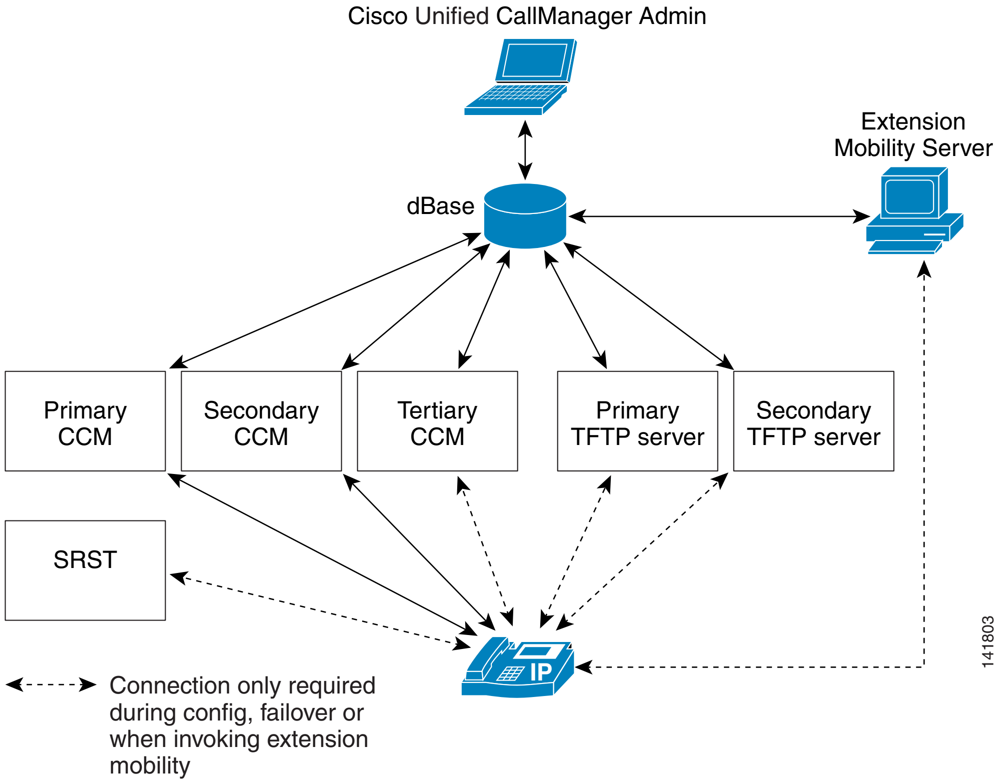

Cisco Unified CallManager Admin
Extension Mobility Server
dBase
Primary CCM
Secondary CCM
Tertiary CCM
Primary TFTP server
Secondary TFTP server
SRST
IP
Connection only required during config, failover or when invoking extension mobility
141803

Figure 41-4 shows a simplified example of a Cisco Unified CallManager B2BUA network. There is a main site and a branch office deployment. Each site has a mixture of SIP and SCCP phones. The main site contains the Cisco Unified CallManager cluster and Voice Mail server. Each phone at the main site and the branch office site are homed to a set of primary, secondary, and tertiary Cisco Unified CallManagers. This provides redundancy of call control in the event of the failure of an individual Cisco Unified CallManager server.

SIP phones at the main site direct all session invitations to Cisco Unified CallManager. Based on routing configuration and destination, Cisco Unified CallManager will either extend a call locally to another SIP or SCCP phone, through the main site voice gateway across the IP WAN to one of the phones in the branch office, or through the main site voice gateway to the PSTN. Calls originating from phones in the branch office are routed similarly with the added ability of routing calls to the PSTN through the branch office voice gateway.

The branch office has an SRST gateway deployed for access to the main site IP WAN and for PSTN access. SIP phones in the branch office will direct all session invitations to the Cisco Unified CallManager at the main site. Similarly to the phones at the main site, Cisco Unified CallManager may extend the call to a phone at the main site, through the main site voice gateway across the IP WAN to a phone in the branch office, or to the PSTSN. Depending on the routing configuration of the Cisco Unified CallManager cluster, PSTN calls originating from the phones in the branch office can be routed to the PSTN through the gateway at the main site or they can be routed locally to the PSTN through the branch office gateway.

The SRST gateway also acts as a backup call control server in the event of an IP WAN outage. Both the SIP and SCCP phones will failover to the SRST gateway during a WAN failure. By doing so, the phones in the branch office are able to have their calls routed by the SRST gateway. This includes calls originating and terminating within the branch office and calls originating and terminating in the PSTN.

SIP Line Side Overview

The SIP line side feature affects Cisco Unified CallManager architecture, the TFTP server, and the Cisco Unified IP Phones. The SIP phone features are equivalent to the SCCP phone features and behave similarly. Cisco SIP IP Phones 7941/61/71/70/11 will support all features. Cisco SIP phones 7905/12/40/60 support a reduced feature set (for example, limited MOH and failover capabilities). SIP trunk side applications work for both SCCP and SIP phones.

For detailed information on the SIP phone features capabilities, refer to the user guide for the specific Cisco SIP phone.

SIP Standards

The following SIP standards are supported in Cisco Unified CallManager:

- RFC3261, RFC3262 (PRACK), RFC3264 (offer/answer), RFC3311 (UPDATE), 3PCC, page 41-15
- RFC3515 (REFER) also Replaces and Referred-by Headers, page 41-16
- Remote Party Id (RPID) Header, page 41-16
- Diversion Header, page 41-16
- Replaces Header, page 41-16
- Join Header, page 41-16
- RFC3265 + Dialog Package, page 41-17
- RFC3265 + Presence Package, page 41-17
- RFC3265 + KPML Package, page 41-17
- RFC3265 + RFC3842 MWI Package (unsolicited notify), page 41-17
- Remotecc, page 41-17
- RFC4028 Session Timers, page 41-17

RFC3261, RFC3262 (PRACK), RFC3264 (offer/answer), RFC3311 (UPDATE), 3PCC

This SIP standard supports the following Cisco Unified CallManager features:

- Basic Call
- Hold and Resume
- Music on Hold
- Distinctive Ringing
- Speed dialing
- Abbreviated Dialing
- Call Forwarding (e.g. 486 and 302 support)
- Meet-me
- Pickup, Group Pickup, Other Group Pickup
- 3 way calling (local SIP phone mixing)

- Parked Call Retrieval
- Shared line: Basic Call

RFC3515 (REFER) also Replaces and Referred-by Headers

These SIP standards support the following Cisco Unified CallManager features:

- Consultative Transfer
- Early Attended Transfer
- Blind Transfer

Remote Party Id (RPID) Header

This SIP standard supports the following Cisco Unified CallManager features:

- Calling Line Id (CLID)
- Calling Party Name Id (CNID)
- Dialed Number Id Service (DNIS)
- Call by call Calling Line Id Restriction (call by call CLIR)

RPID is a SIP header used for identification services. RPID is used to indicate the calling, called, and connected remote party information to the other party for identification and call-back, legal intercept, indication of user identification and user location to emergency services, and the identification of users for accounting and billing services.

Diversion Header

This SIP standard supports the following Cisco Unified CallManager features:

- Redirected Number Id Service (RDNIS)
- Call Forward All Activation, Call Forward Busy, Call Forward No Answer

Replaces Header

This SIP standard supports the following Cisco Unified CallManager feature:

- Shared Line: Remote Resume

Join Header

This SIP standard supports the following Cisco Unified CallManager feature:

- Shared Line: Barge

RFC3265 + Dialog Package

This SIP standard supports the following Cisco Unified CallManager feature:

- Shared Line: Remote State Notifications

RFC3265 + Presence Package

These SIP standards support the following Cisco Unified CallManager features:

- BLF on Speed Dial
- BLF on Missed, Placed, Received Calls lists

RFC3265 + KPML Package

These SIP standards support the following Cisco Unified CallManager features:

- Digit Collection
- OOB DTMF

RFC3265 + RFC3842 MWI Package (unsolicited notify)

These SIP standards support the following Cisco Unified CallManager feature:

- Message Waiting Indication

Remotecc

This SIP standard supports the following Cisco Unified CallManager features:

- Adhoc conferencing
- Remove Last Participant
- Conflist
- Immediate Diversion
- Call Park
- Call Select
- Shared Line: Privacy

RFC4028 Session Timers

Allows periodic refresh of the SIP sessions through re-INVITE and allows Cisco Unified CallManager to determine whether the signalling connection to the remote is still active.

Cisco Unified CallManager Functionality Supported by SIP Phones

The following Cisco Unified CallManager functions are supported on Cisco SIP phones:

- Dial Plans, page 41-18
- PLAR, page 41-18
- Softkey Handling, page 41-18
- DSCP Configuration, page 41-19
- SIP Profiles for Endpoints, page 41-19
- Network Time Protocol (NTP), page 41-19

Dial Plans

Unlike the SCCP phones, the SIP phones collect digits locally before sending them to Cisco Unified CallManager. The SIP phones use a local dial plan to know when enough digits have been entered and to trigger an INVITE with the collected digits. SIP phones that are in SRST mode will continue to use any configured dial plans that they receive from Cisco Unified CallManager. See SIP Dial Rules, page 19-4 for more information.

PLAR

Private Line Automatic Ringdown (PLAR) is a term used by traditional telephony systems that refers to a phone configuration whereby any time the user goes off hook, the phone immediately dials a preconfigured number. The user is unable to dial any other numbers from that phone (or line). This is implemented in for SCCP IP phones in Cisco Unified CallManager by using partitions, calling search space (CSS), and translation patterns; neither the device configuration nor line configuration indicates that PLAR is setup for the phone.

Administrators use SIP Dial Rules for configuring PLAR in SIP phones. Phones configured for PLAR will have a one-line dial plan configuration specifying the appropriate target pattern. When the user goes off hook, the phone will populate the INVITE with the target string and immediately send the request to Cisco Unified CallManager. The user does not enter any digits. See Configuring SIP Dial Rules, page 30-3 for more information.

Softkey Handling

The administrator uses Cisco Unified CallManager Administration to modify the softkey sets that the phone displays. Keys can be added, removed, and their positions can be changed. This data gets written to the database and is sent to the SCCP phone via Station messages as part of the phone registration/initialization process. For Cisco SIP phones, however, instead of sending the keys in Station Messages, the Cisco Unified CallManager TFTP server builds the file that contains the softkey sets. The SIP phone retrieves these files from the TFTP server and the new softkey sets overwrites the softkey sets that are built into the phone. This allows Cisco Unified CallManager to modify the default softkeys and also lets Cisco Unified CallManager manipulate the softkey events, so that it can directly control some phone-level features.

For features that are configured by using the Softkey Configuration window but are not supported by the SIP phone, the softkey will be displayed, but the phone will display a message that the key is not active. This is consistent with the SCCP phone behavior.

The Dial softkey appears as part of the default softkey set when the SIP phone is operating in SRST mode.

Note The Cisco SIP IP Phones 7905, 7912, 7940, and 7960 do not download softkeys. These phones get their softkey configuration in the phone firmware.

DSCP Configuration

Cisco SIP phones get their DSCP information from the configuration file that gets downloaded to the device. The DSCP setting is for the device; whereas, the SCCP phones can get the DSCP setting for a call. DSCP values get configured in the Enterprise Parameters Configuration window, and in the Cisco Unified CallManager Service Parameters Configuration window.

SIP Profiles for Endpoints

Because SIP attributes rarely change, Cisco Unified CallManager uses SIP profiles to define SIP attributes that are associated with SIP trunks and Cisco SIP IP phones. Having these attributes in a profile instead of adding them individually to every SIP trunk and SIP phone decreases the amount of time administrators spend configuring SIP devices and allows the administrator to change the values for a group of devices. Because the SIP profile is a required field when configuring SIP trunks and phones, Cisco Unified CallManager provides a default SIP; however, administrators can create customized SIP profiles. SIP profiles get assigned to SIP devices by using Cisco Unified CallManager Administration.

The software on the SIP phone uses the majority of SIP values that are sent via TFTP to the phones.

For information on configuring SIP profiles, see Configuring SIP Profiles in the *Cisco Unified CallManager Administration Guide*.

Network Time Protocol (NTP)

You can configure phone Network Time Protocol (NTP) references in Cisco Unified CallManager Administration to ensure that a Cisco SIP IP Phone gets its date and time from the NTP server. If all NTP servers do not respond, then the SIP phone uses the date header in the 200 OK response to the REGISTER message for the date and time.

After you add the phone NTP reference to Cisco Unified CallManager Administration, you must add it to a date/time group. In the date/time group, you prioritize the phone NTP references, starting with the first server that you want the phone to contact.

The date/time group configuration gets specified in the device pool, and the device pool gets specified on the phone page.

For information on configuring the NTP reference, see Phone NTP Reference Configuration in the *Cisco Unified CallManager Administration Guide*.

Where to Find More Information

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design*

Related Topics

- Caller Identification and Restriction, page 17-28
- Understanding IP Telephony Protocols, page 40-1
- SIP Networks, page 41-1
- SIP and Cisco Unified CallManager, page 41-2
- SIP Functions That Are Supported in Cisco Unified CallManager, page 41-5
- SIP Trunk Configuration Checklist, page 41-13
- Understanding Cisco Unified CallManager Trunk Types, page 42-1
- Trunk Configuration, *Cisco Unified CallManager Administration Guide*
- SIP Dial Rules Configuration, *Cisco Unified CallManager Administration Guide*
- SIP Profile Configuration, *Cisco Unified CallManager Administration Guide*

Understanding Cisco Unified CallManager Trunk Types

In a distributed call-processing environment, Cisco Unified CallManager communicates with other Cisco Unified CallManager clusters, the public switched telephone network (PSTN), and other non-IP telecommunications devices, such as private branch exchanges (PBXs) by using trunk signaling protocols and voice gateways.

This section covers the following topics:

- Cisco Unified CallManager Trunk Configuration, page 42-1
- Trunks and Gatekeepers in Cisco Unified CallManager, page 42-2
- Trunk Types in Cisco Unified CallManager Administration, page 42-2
- Dependency Records for Trunks and Associated Route Groups, page 42-6
- Trunk Configuration Checklist, page 42-6
- Where to Find More Information, page 42-7

Cisco Unified CallManager Trunk Configuration

Trunk configuration in Cisco Unified CallManager Administration depends on the network design and call-control protocols that are used in the IP WAN. All protocols require that either a signaling interface (trunk) or a gateway be created to accept and originate calls. For some IP protocols, such as MGCP, you configure trunk signaling on the gateway. You specify the type of signaling interface when you configure the gateway in Cisco Unified CallManager. For example, to configure QSIG connections to Cisco Unified CallManager, you must add an MGCP voice gateway that supports QSIG protocol to the network. You then configure the T1 PRI or E1 PRI trunk interface to use the QSIG protocol type. For more information about configuring gateways, see the "Understanding Cisco Unified CallManager Voice Gateways" chapter.

Related Topics

- Trunks and Gatekeepers in Cisco Unified CallManager, page 42-2
- Trunk Types in Cisco Unified CallManager Administration, page 42-2

Trunks and Gatekeepers in Cisco Unified CallManager

In addition to using gateways to route calls, you can configure trunks in Cisco Unified CallManager Administration to function in either of the following ways:

- Gatekeeper-Controlled Trunks, page 42-2
- Non-Gatekeeper-Controlled Trunks, page 42-2

Gatekeeper-Controlled Trunks

Gatekeepers that are used in a distributed call-processing environment provide call routing and call admission control for Cisco Unified CallManager clusters. Intercluster trunks that are gatekeeper-controlled can communicate with all remote clusters. Similarly, an H.225 trunk can communicate with any H.323 gatekeeper-controlled endpoints including Cisco Unified CallManager clusters. Route patterns or route groups can route the calls to and from the gatekeeper. In a distributed call-processing environment, the gatekeeper uses the E.164 address (phone number) and determines the appropriate IP address for the destination of each call, and the local Cisco Unified CallManager uses that IP address to complete the call.

For large distributed networks where many Cisco Unified CallManager clusters exist, you can avoid configuring individual intercluster trunks between each cluster by using gatekeepers.

When you configure gatekeeper-controlled trunks, Cisco Unified CallManager creates a virtual trunk device. The gatekeeper changes the IP address of this device dynamically to reflect the IP address of the remote device. Specify these trunks in the route patterns or route groups that route calls to and from the gatekeeper.

Refer to the *Cisco Unified Communications Solution Reference Network Design* guide for more detailed information about gatekeeper configuration, dial plan considerations when using a gatekeeper, and gatekeeper interaction with Cisco Unified CallManager.

Non-Gatekeeper-Controlled Trunks

With no gatekeepers in the distributed call-processing environment, you must configure a separate intercluster trunk for each remote device pool in a remote cluster that the local Cisco Unified CallManager can call over the IP WAN. You also configure the necessary route patterns and route groups to route calls to and from the various intercluster trunks. The intercluster trunks statically specify the IP addresses of the remote devices.

Related Topics

- Trunk Types in Cisco Unified CallManager Administration, page 42-2
- Trunk Configuration Checklist, page 42-6

Trunk Types in Cisco Unified CallManager Administration

Your choices for configuring trunks in Cisco Unified CallManager depend on whether the IP WAN uses gatekeepers to handle call routing. Also, the types of call-control protocols that are used in the call-processing environment determine trunk configuration options.

You can configure these types of trunk devices in Cisco Unified CallManager Administration:

- H.225 Trunk (Gatekeeper Controlled), page 42-3
- Intercluster Trunk (Gatekeeper Controlled), page 42-3
- Intercluster Trunk (Non-Gatekeeper Controlled), page 42-3
- SIP Trunk, page 42-3

H.225 Trunk (Gatekeeper Controlled)

In an H.323 network that uses gatekeepers, use an H.225 trunk with gatekeeper control to configure a connection to a gatekeeper for access to other Cisco Unified CallManager clusters and to H.323 devices. An H.225 trunk can communicate with any H.323 gatekeeper-controlled endpoint. When you configure an H.323 gateway with gatekeeper control in Cisco Unified CallManager Administration, use an H.225 trunk. To choose this method, use **Device** > **Trunk** and choose **H.225 Trunk (Gatekeeper Controlled)**.

You also configure route patterns and route groups to route calls to and from the gatekeeper. For more information about, see the "Gatekeepers and Trunks" section on page 8-6.

Intercluster Trunk (Gatekeeper Controlled)

In a distributed call-processing network with gatekeepers, use an intercluster trunk with gatekeeper control to configure connections between clusters of Cisco Unified CallManager systems. Gatekeepers provide call admission control and address resolution for intercluster calls. A single intercluster trunk can communicate with all remote clusters. To choose this method, use **Device** > **Trunk** and choose **Inter-Cluster Trunk (Gatekeeper Controlled)** in Cisco Unified CallManager Administration.

You also configure route patterns and route groups to route the calls to and from the gatekeeper. In this configuration, the gatekeeper dynamically determines the appropriate IP address for the destination of each call, and the local Cisco Unified CallManager uses that IP address to complete the call

For more information about gatekeepers, see the "Gatekeepers and Trunks" section on page 8-6.

Intercluster Trunk (Non-Gatekeeper Controlled)

In a distributed network that has no gatekeeper control, you must configure a separate intercluster trunk for each device pool in a remote cluster that the local Cisco Unified CallManager can call over the IP WAN. The intercluster trunks statically specify the IP addresses or host names of the remote devices.To choose this method, use **Device** > **Trunk** and choose **Inter-Cluster Trunk (Non-Gatekeeper Controlled)** in Cisco Unified CallManager Administration.

Note You must specify the IP addresses of all remote Cisco Unified CallManager nodes that belong to the device pool of the remote non-gatekeeper-controlled intercluster trunk.

You also configure the necessary route patterns and route groups to route calls to and from the intercluster trunks.

SIP Trunk

In a call-processing environment that uses Session Initiation Protocol (SIP), use SIP trunks to configure a signaling interface with Cisco Unified CallManager for SIP calls. SIP trunks (or signaling interfaces) connect Cisco Unified CallManager clusters with a SIP proxy server. A SIP signaling interface uses port-based routing, and Cisco Unified CallManager accepts calls from any gateway as long as the SIP messages arrive on the port that is configured as a SIP signaling interface. The SIP signaling interface uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more endpoints.

To choose this method, use **Device** > **Trunk** and choose **SIP Trunk** in Cisco Unified CallManager Administration.

You must also configure route groups and route patterns that use the SIP trunks to route the SIP calls.

For more information about SIP and configuring SIP trunks, see the "SIP and Cisco Unified CallManager" section on page 41-2.

Related Topics

- Trunk Configuration Checklist, page 42-6
- Dependency Records for Trunks and Associated Route Groups, page 42-6

Transferring Calls Between Trunks

Using Cisco Unified CallManager Administration, you can configure trunks as OnNet (internal) trunks or OffNet (external) trunks by using Trunk Configuration or by setting a clusterwide service parameter. Used in conjunction with the clusterwide service parameter, Block OffNet to OffNet Transfer, the configuration determines whether calls can be transferred over a trunk.

To use the same trunk to route both OnNet and OffNet calls, associate the trunk with two different route patterns. Make one trunk OnNet and the other OffNet with both having the Allow Device Override check box unchecked.

Configuring Transfer Capabilities Using Trunk Configuration

Using Cisco Unified CallManager Administration Trunk Configuration, you can configure a trunk as OffNet or OnNet. The calls coming to the network through that trunk are considered OffNet or OnNet, respectively. Use the Trunk Configuration window field, Call Classification, to configure the trunk as OffNet, OnNet, or Use System Default. See Table 42-1 for description of these settings.

The Route Pattern Configuration window provides a drop-down list box called Call Classification, which allows you to configure a route pattern as OffNet or OnNet. When Call Classification is set to OffNet and the Allow Device Override check box is unchecked, the system considers the outgoing calls that use this route pattern as OffNet (if configured as OnNet and check box is unchecked, then outgoing calls are considered OnNet).

The same trunk can be used to route both OnNet and OffNet calls by associating the trunk with two different route patterns: one OnNet and the other OffNet, with both having the Allow Device Override check box unchecked. For outgoing calls, the outgoing device setting classifies the call as either OnNet or OffNet by determining if the Allow Device Override check box is checked.

In route pattern configuration, if the Call Classification is set as OnNet, the Allow Device Override check box is checked, and the route pattern is associated with an OffNet Trunk, the outgoing call is considered OffNet.

Table 42-1 Trunk Configuration Call Classification Settings

Setting Name	Description
OffNet	This setting identifies the trunk as being an external trunk. When a call comes in from a trunk that is configured as OffNet, the outside ring gets sent to the destination device.
OnNet	This setting identifies the trunk as being an internal trunk. When a call comes in from a trunk that is configured as OnNet, the inside ring gets sent to the destination device.
Use System Default	This setting uses the Cisco Unified CallManager clusterwide service parameter Call Classification.

Configuring Transfer Capabilities by Using Call Classification Service Parameter

To configure all trunks to be OffNet (external) or OnNet (internal), perform the following two steps:

1. Use the Cisco Unified CallManager clusterwide service parameter Call Classification.
2. Configure individual trunks to Use System Default in the Call Classification field that is on the Trunk Configuration window.

Blocking Transfer Capabilities by Using Service Parameters

Block transfer restricts the transfer between external devices, so fraudulent activity gets prevented. You can configure the following devices as OnNet (internal) or OffNet (external) to Cisco Unified CallManager:

- H.323 gateway
- MGCP FXO trunk
- MGCP T1/E1 trunk
- Intercluster trunk
- SIP trunk

If you do not want OffNet calls to be transferred to an external device (one that is configured as OffNet), set the Cisco Unified CallManager clusterwide service parameter, Block OffNet to OffNet Transfer, to True.

If a user tries to transfer a call on an OffNet trunk that is configured as blocked, a message displays on the user phone to indicate that the call cannot be transferred.

Related Topics

- Route Pattern Configuration, *Cisco Unified CallManager Administration Guide*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide*
- Trunk Configuration, *Cisco Unified CallManager Administration Guide*

Dependency Records for Trunks and Associated Route Groups

To find route groups that use a specific trunk, click the Dependency Records link that is provided on the Cisco Unified CallManager Administration Trunk Configuration window. The Dependency Records Summary window displays information about route groups that are using the trunk. To find out more information about the route group, click the route group, 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 Unified CallManager Administration Guide*.

Related Topics

- Trunk Configuration Checklist, page 42-6
- Trunk Types in Cisco Unified CallManager Administration, page 42-2

Trunk Configuration Checklist

Table 42-2 provides an overview of the steps that are required to configure trunk interfaces in Cisco Unified CallManager, along with references to related procedures and topics.

Table 42-2 Trunk Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Gather the endpoint information, such as IP addresses or host names, that you need to configure the trunk interface.	*Cisco Unified Communications Solution Reference Network Design*
Step 2	For gatekeeper-controlled trunks, configure the gatekeeper. For SIP trunks, perform proxy configuration.	Gatekeeper and Trunk Configuration Checklist, page 8-10 SIP Trunk Configuration Checklist, page 41-13
Step 3	Add the appropriate trunks in Cisco Unified CallManager Administration. • H.225 trunks (gatekeeper controlled) • Intercluster trunks (gatekeeper controlled) • Intercluster trunks (non-gatekeeper controlled) • SIP trunks	Configuring a Trunk, *Cisco Unified CallManager Administration Guide* Trunk Configuration Settings, *Cisco Unified CallManager Administration Guide* SIP Trunk Configuration Checklist, page 41-13
Step 4	Configure the gatekeeper-controlled intercluster trunks or H.225 trunks to specify gatekeeper information. Configure the non-gatekeeper-controlled trunks with the IP address or host name for the remote Cisco Unified CallManager server.	Trunk Configuration Settings, *Cisco Unified CallManager Administration Guide*

Table 42-2 Trunk Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 5	Configure a route pattern or route group to route calls to each gatekeeper-controlled trunk. Configure a route pattern or route group to route calls to each non-gatekeeper-controlled trunk.	Route Pattern Configuration,*Cisco Unified CallManager Administration Guide* Route Group Configuration, *Cisco Unified CallManager Administration Guide* SIP Trunk Configuration Checklist, page 41-13
Step 6	Reset the trunk interface to apply the configuration settings.	Resetting a Trunk, *Cisco Unified CallManager Administration Guide*

Related Topics

- Cisco Unified CallManager Trunk Configuration, page 42-1
- Trunks and Gatekeepers in Cisco Unified CallManager, page 42-2
- Trunk Types in Cisco Unified CallManager Administration, page 42-2
- Dependency Records for Trunks and Associated Route Groups, page 42-6

Where to Find More Information

Related Topics

- Gatekeepers and Trunks, page 8-6
- Cisco Voice Gateways, page 39-1
- Gateways, Dial Plans, and Route Groups, page 39-12
- Understanding Session Initiation Protocol (SIP), page 41-1
- Trunk Configuration, *Cisco Unified CallManager Administration Guide*
- Gatekeeper Configuration, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design*
- *Cisco ICS 7750 System Description*
- *Configuring Cisco Unified Communications Voice Gateways*

CHAPTER 43

Cisco Unified IP Phones

Cisco Unified IP Phones as full-featured telephones can plug directly into your IP network. H.323 clients, CTI ports, and Cisco IP Communicator comprise software-based devices that you configure similarly to the Cisco Unified IP Phones. Cisco Unified CallManager Administration allows you to configure phone features such as call forwarding and call waiting for your phone devices. You can also create phone button templates to assign a common button configuration to a large number of phones.

After you have added the phones, you can associate users with them. By associating a user with a phone, you give that user control over that device.

This section covers the following topics:

- Supported Cisco Unified IP Phones, page 43-2
- Cisco SIP IP Phones, page 43-7
- H.323 Clients and CTI Ports, page 43-8
- Cisco IP Communicator, page 43-8
- Cisco Unified Personal Communicator, page 43-8
- Phone Button Templates, page 43-9
- Softkey Templates, page 43-15
- Softkey Template Operation, page 43-18
- Common Phone Profiles, page 43-19
- Methods for Adding Phones, page 43-19
- Phone Features, page 43-20
- Phone Association, page 43-25
- Phone Administration Tips, page 43-25
- Phone Failover and Fallback, page 43-29
- Phone Configuration Checklist, page 43-29
- Where to Find More Information, page 43-33

Supported Cisco Unified IP Phones

Table 43-1 provides an overview of the features that are available on the following Cisco Unified IP Phones that Cisco Unified CallManager supports:

- Cisco Unified IP Phone model 7900 family (SCCP and SIP protocols)
- Cisco Unified IP Video Phone model 7985
- Cisco Unified IP Phone model 7914 Expansion Module
- Cisco IP Conference Station 7935 and 7936
- Cisco IP Phone model 30 VIP
- Cisco IP Phone model 12 series

For the latest information on features and services that these phone models support, refer to the following documentation:

- Phone administration or user documentation that supports the phone model and this version of Cisco Unified CallManager
- Firmware release notes for your phone model
- Cisco Unified CallManager release notes

Table 43-1 Supported Cisco Unified IP Phones and Features

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7970 and Cisco Unified IP Phone 7971	The Cisco Unified IP Phone models 7970 and 7971, full-featured, eight-line business sets, support the SCCP and SIP protocols and the following features: • A backlit, color touchscreen display for easy access to call details and features. • Four fixed feature buttons: – Messages—accessing voice-messaging messages – Settings—adjusting phone settings – Services—accessing services – Directories—accessing call logs and directories • A Help (?) button for immediate assistance with calling features • Eight programmable buttons to use as line buttons, speed-dial buttons, or for other phone services • Five softkeys for accessing additional call details and functionality (Softkeys change depending on the call state for a total of 16 softkeys.) • An internal, two-way, full-duplex speakerphone and microphone mute The Cisco Unified IP Phone models 7970/71G-GE represent the gigabit ethernet version of the Cisco Unified IP Phone models 7970/71 while Cisco Unified IP Phone models 7970G, 7960G and 7940G represent the non-gigabit version.

Table 43-1 Supported Cisco Unified IP Phones and Features (continued)

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7960 and Cisco Unified IP Phone 7961	The Cisco Unified IP Phone models 7960 and 7961, full-featured, six-line business sets, support the SCCP and SIP protocols and the following features: • A help (*?*) button • Six programmable buttons to use as line, speed-dial, or feature buttons • Four fixed buttons for accessing voice-messaging messages, adjusting phone settings, accessing services, and accessing directories • Four softkeys for accessing additional call details and functionality (Softkeys change depending on the call state for a total of 16 softkeys.) • A large LCD display that shows call details and softkey functions • An internal, two-way, full-duplex speakerphone and microphone mute
Cisco Unified IP Phone 7940 and Cisco Unified IP Phone 7941	The Cisco Unified IP Phone models 7940 and 7941, two-line business sets with features similar to the Cisco Unified IP Phone model 7960, support the SCCP and SIP protocols and include the following features: • A help (*?*) button • Two programmable buttons to use as line, speed-dial, or feature buttons • Four fixed buttons for accessing voice-messaging messages, services, and directories, and for adjusting phone settings • Four softkeys for accessing additional call details and functionality (Softkeys change depending upon the call state for a total of 16 softkeys.) • A large LCD display that shows call details and softkey functions • An internal, two-way, full-duplex speakerphone and microphone mute

Table 43-1 Supported Cisco Unified IP Phones and Features (continued)

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7920	The Cisco Wireless IP Phone model 7920, which is an easy-to-use IEEE 802.11b wireless IP phone, provides comprehensive voice communication in conjunction with Cisco Unified CallManager and Cisco Aironet (r) 1200, 1100, 350, and 340 series of Wi-Fi (IEEE 802.11b) access points. Features include • A pixel-based display for intuitive access to calling features • Two soft keys that dynamically present calling options to the user • A four-way rocker switch that allows easy movement through the displayed information • Volume control for easy decibel-level adjustments of the handset and ringer when in use
Cisco Unified IP Phone 7914 Expansion Module	Cisco Unified IP Phone model 7914 Expansion Module extends the functionality of the Cisco Unified IP Phone model 7960 by providing 14 additional buttons. To configure these buttons as line or speed dials, use Phone Button Template Configuration. **Note** You can create the Cisco Unified IP Phone model 7914 Expansion Module phone button template by renaming the phone button template that is used for the standard Cisco Unified IP Phone model 7960. Refer to "Phone Button Template Configuration" in the *Cisco Unified CallManager Administration Guide* for more information. The Cisco Unified IP Phone model 7914 Expansion Module includes an LCD to identify the function of the button and the line status. You can daisy chain two Cisco Unified IP Phone model 7914 Expansion Modules to provide 28 additional lines or speed-dial and feature buttons.
Cisco Unified IP Phone 7912	The Cisco Unified IP Phone model 7912, which is a single-line phone that supports a maximum of two calls at the same time, supports the SCCP and SIP protocols and provides basic-feature functionality for individuals who conduct low to medium telephone traffic. This model, which supports inline power, provides an integrated 10/100 Ethernet switch for connectivity to a collocated PC. This model offers four dynamic softkeys.

Table 43-1 Supported Cisco Unified IP Phones and Features (continued)

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7911	The Cisco Unified IP Phone model 7911, which is a single-line phone that supports a maximum of two calls at the same time, supports the SCCP and SIP protocols and provides basic-feature functionality for individuals who conduct low to medium telephone traffic. The Cisco Unified IP Phone model 7911 menus are similar to the Cisco Unified IP Phone 7970. The Applications Menu button opens up a main applications menu. This model, which supports inline power, provides an integrated 10/100 Ethernet switch for connectivity to a collocated PC. This model offers four dynamic softkeys.
Cisco Unified IP Phone 7910	The Cisco Unified IP Phone model 7910, a single-line, basic-feature phone that is designed primarily for common-use areas with medium telephone traffic such as lobbies or breakrooms, includes the following features: • Four dedicated feature buttons for Line, Hold, Transfer, and Settings • Six programmable feature buttons that you can configure through phone button templates in Cisco Unified CallManager Available features include Call Park, Redial, Speed Dial, Call Pickup, Conference, Forward All, Message Waiting, and Meet-Me Conference. • A two-line LCD display (24 characters per line) that indicates the directory number, call status, date, and time • An internal speaker that is designed for hands-free dialing.
Cisco Unified IP Phone 7905	The Cisco Unified IP Phone model 7905, a low-cost, single-line, basic-feature phone that is designed primarily for common-use areas such as cafeterias, break rooms, lobbies, and manufacturing floors, supports the SCCP and SIP protocols and includes the following features: • LCD that displays features such as time, date, phone number, caller ID, call status, and softkey tabs • Four softkeys that engage the function that displays on the corresponding LCD screen tabs. (Softkey functions change depending on the status of the phone.) • Three dedicated buttons for Hold, Menu, and Navigation • An internal speaker that is designed for hands-free dialing

Table 43-1 Supported Cisco Unified IP Phones and Features (continued)

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone model 7902	The Cisco Unified IP Phone model 7902 provides a cost-effective, entry-level IP phone for a lobby, laboratory, manufacturing floor, or another area where only basic calling capability is required. The single-line Cisco Unified IP Phone model 7902 includes the following features: • Fixed feature keys that provide one-touch access to the redial, transfer, conference, and voice-messaging access features • Three dedicated buttons for hold, menu, and volume control • Inline power that allows the phone to receive power over the LAN
Cisco Unified IP Phone 7985	The Cisco Unified IP Phone model 7985G provides business-quality video over the same data network that your computer uses. The video phone provides the same softkey functionality and features as a Cisco IP telephone, which allows you to place and receive calls, put calls on hold, transfer calls, make conference calls, and so on. The Cisco Unified IP Phone model 7985G provides the following features: • Color screen • Support for up to eight line or speed-dial numbers • Context-sensitive online help for buttons and feature
Cisco Unified IP Conference Station 7936	The Cisco Unified IP Conference Station 7936, a full-featured, IP-based, hands-free conference station for use on desktops, in offices, and in small-to medium-sized conference rooms, includes the following features: • Three softkeys and menu navigation keys that guide a user through call features and functions including available features Call Park, Call Pick Up, Group Call Pick Up, Transfer, and Conference (Ad Hoc and Meet-Me). • An LCD display that indicates the date and time, calling party name, calling party number, digits dialed, feature, and line status • A digitally tuned speaker and three microphones that allow conference participants to move around while speaking • Microphone mute • Ability to add external microphones to support larger rooms

Table 43-1 Supported Cisco Unified IP Phones and Features (continued)

Cisco Unified IP Phone Model	Description
Cisco IP Conference Station 7935	The Cisco IP Conference Station 7935, a full-featured, IP-based, hands-free conference station for use on desktops, in offices and in small-to medium-sized conference rooms, includes the following features: • Three softkeys and menu navigation keys that guide a user through call features and functions Available features include Call Park, Call Pick Up, Group Call Pick Up, Transfer, and Conference (Ad Hoc and Meet-Me). • An LCD display that indicates the date and time, calling party name, calling party number, digits dialed, feature, and line status • A digitally tuned speaker and three microphones that allow conference participants to move around while speaking • Microphone mute
Cisco IP Phone 12 SP+	The Cisco IP Phone model 12 SP+ offers many of the same features as PBX or POTS telephones. This IP phone includes the following features: • 12 programmable line and feature buttons • An LED that is associated with each of the 12 feature and line buttons to indicate feature and line status • A two-line LCD display (20 characters per line) for call status and identification • An internal, two-way speakerphone and microphone mute
Cisco IP Phone 30 VIP	The Cisco IP Phone model 30 VIP offers many of the same features as PBX or POTS telephones. This IP phone includes the following features: • 26 programmable line and feature buttons • An LED that is associated with each of the 26 feature and line buttons to indicate feature and line status • A two-line LCD for displaying date and time, calling party name, calling party number, and digits dialed • An internal, two-way speakerphone with microphone mute • Dedicated feature buttons for Transfer, Hold, and Redial

Cisco SIP IP Phones

Cisco Unified CallManager supports the SIP protocol on the following Cisco Unified IP Phone models:

- Cisco Unified IP Phone 7970/71
- Cisco Unified IP Phone 7960/61
- Cisco Unified IP Phone 7940/41

- Cisco Unified IP Phone 7911
- Cisco Unified IP Phone 7905/12

The administrator uses the Cisco Unified CallManager Administration Phone Configuration window to configure an IP Phone for SCCP or SIP. If SIP is chosen, additional Cisco Unified CallManager Administration configuration windows get used to configure the SIP protocol; for example, SIP Profile Configuration. See Table 43-6 for configuration requirements. For information on SIP Profiles and SIP Dial Rules, see SIP Dial Rules Configuration and SIP Profile Configuration in the *Cisco Unified CallManager Administration Guide.*

H.323 Clients and CTI Ports

Cisco Unified CallManager Administration enables you to configure software-based devices such as H.323 clients and CTI ports. Software-based Cisco Unified CallManager applications such as Cisco SoftPhone, Cisco AutoAttendant, and Cisco IP Interactive Voice Response (IVR) use CTI ports that are virtual devices.

H.323 clients include Microsoft NetMeeting devices.

You configure H.323 clients and CTI ports through the Phone Configuration window in Cisco Unified CallManager Administration like you do phones, but they often require fewer configuration settings.

Note Cisco recommends that you do not configure CTI ports or devices that use TAPI applications in a line group.

For information on H.323 clients and shared line appearances, see the "Shared Line Appearance" section on page 18-2.

For instructions on how to configure H.323 clients and CTI ports, refer to "Cisco Unified IP Phone Configuration" in the *Cisco Unified CallManager Administration Guide*.

Cisco IP Communicator

Cisco IP Communicator, a software-based application, allows users to place and receive phone calls by using their personal computers. Cisco IP Communicator depends upon the Cisco Unified CallManager call-processing system to provide telephony features and voice-over-IP capabilities.

This interaction with Cisco Unified CallManager means that Cisco IP Communicator provides the same functionality as a full-featured Cisco Unified IP Phone, while providing the portability of a desktop application. Additionally, it means that you administer Cisco IP Communicator as a phone device by using the Cisco Unified CallManager Administration Phone Configuration window.

Cisco Unified Personal Communicator

Cisco Unified Personal Communicator, a desktop software application, provides access to voice, video, document-sharing and presence applications – all from a single, rich media interface. Cisco Unified Personal Communicator relies on the Cisco Unified CallManager call-processing system to provide telephony features and voice-over-IP capabilities.

This interaction with Cisco Unified CallManager enables Cisco Unified Personal Communicator to offer integrated softphone capabilities and control of the user's physical IP phone. Additionally, it means you administer Cisco Unified Personal Communicator as a phone device by using the Cisco Unified CallManager Administration Phone Configuration window.

Phone Button Templates

Cisco Unified CallManager includes several default phone button templates. When adding phones, you can assign one of these templates to the phones or create a new template.

Creating and using templates provides a fast way to assign a common button configuration to a large number of phones. For example, if users in your company do not use the conference feature, you can create a template that reassigns this button to a different feature, such as speed dial.

To create a template, you must make a copy of an existing template and assign the template a unique name. You can make changes to the custom templates that you created, and you can change the labels of the default phone button templates. You cannot change the function of the buttons in the default templates. You can rename existing templates and modify them to create new ones, update custom templates to add or remove features, lines, or speed dials, and delete custom templates that are no longer being used. When you update a template, the change affects all phones that use the template.

Renaming a template does not affect the phones that use that template. All Cisco Unified IP Phones that use this template continue to use this template after it is renamed.

Make sure that all phones have at least one line that is assigned to each phone. Normally, this assignment specifies button 1. Phones can have additional lines that are assigned, depending on the Cisco Unified IP Phone model. Phones also generally have several features, such as speed dial, that are assigned to the remaining buttons.

You can delete phone templates that are not currently assigned to any phone in your system if they are not the only template for a given phone model. You cannot delete a template that is assigned to one or more devices or the default template for a model (specified in the Device Defaults Configuration window). You must reassign all Cisco Unified IP Phones that are using the template that you want to delete to a different phone button template before you can delete the template.

Note The standard phone button template for the Cisco Unified IP Phone model 7960, which supports the Cisco Unified IP Phone model 7914 Expansion Module, includes buttons for both devices (up to 34 buttons).

Choose Dependency Records from the Related Links drop-down list box on the Phone Button Template Configuration window to view the devices that are using a particular template.

Cisco Unified CallManager does not directly control all features on Cisco Unified IP Phones through phone button templates. Refer to the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager* and other phone documentation for detailed information about individual Cisco Unified IP Phone 7900 family models.

Default Phone Button Templates

Although all Cisco Unified IP Phones support similar features, you implement these features differently on various models. For example, some models configure features such as Hold or Transfer by using phone button templates; other models have fixed buttons or onscreen program keys for these features that are not configurable. Also, the maximum number of lines or speed dials that are supported differs for some phone models. These differences require different phone button templates for specific models.

Each Cisco Unified IP Phone model comes with a default phone button template. You can use the default templates as is to quickly configure phones. You can also copy and modify the templates to create custom templates.

Custom templates enable you to make features available on some or all phones, restrict the use of certain features to certain phones, configure a different number of lines or speed dials for some or all phones, and so on, depending on how the phone will be used. For example, you may want to create a custom template that can be applied to phones that will be used in conference rooms. Table 43-2 provides descriptions of the standard phone button templates.

Table 43-2 Default Phone Button Templates Listed by Model

Phone Button Template Name	Template Description
Standard 7985	The Standard 7985 template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco IP Video Phone 7985.
Standard 7971 SCCP	The Standard 7971 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7971.
Standard 7971 SIP	The Standard 7971 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7971.
Standard 7970 SCCP	The Standard 7970 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7970.
Standard 7970 SIP	The Standard 7970 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7970.

Table 43-2 Default Phone Button Templates Listed by Model (continued)

Phone Button Template Name	Template Description
Standard 7961 SCCP and Standard 7961G-GE SCCP	The Standard 7961 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7961.
Standard 7961 SIP	The Standard 7961 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7961.
Standard 7960 SCCP	The Standard 7960 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7960.
Standard 7960 SIP	The Standard 7960 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7960.
Standard 7941 SCCP and Standard 7941G-GE SCCP	The Standard 7941 SCCP template comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7941.
Standard 7941 SIP	The Standard 7940 SIP template comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7941.
Standard 7940 SCCP	The Standard 7940 SCCP templates comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7940.
Standard 7940 SIP	The Standard 7940 SIP template comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7940.
Standard 7920	The Standard 7920 template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 for speed dials.

Table 43-2 Default Phone Button Templates Listed by Model (continued)

Phone Button Template Name	Template Description
Standard 7912 SCCP	The Standard 1912 SCCP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7912 SIP	The Standard 7912 SIP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7911 SCCP	The Standard 7911 SCCP template uses button 1 for line 1, makes button 2 configurable (default specifies None), and assigns buttons 3 through 6 as speed dials. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7911.
Standard 7911 SIP	The Standard 7911 SIP template uses button 1 for line 1, makes button 2 configurable (default specifies None), and assigns buttons 3 through 6 as speed dials. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7911.
Standard 7910	The Standard 7910 template uses button 1 for message waiting, button 2 for conference, button 3 for forwarding, buttons 4 and 5 for speed dial, and button 6 for redial. The Cisco Unified IP Phone 7910 includes fixed buttons for Line, Hold, Transfer, and Settings.
Standard 7905 SCCP	The Standard 7905 SCCP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7905 SIP	The Standard 7905 SIP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7902	The Standard 7902 template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7936	The Standard 7936 template, which is not configurable for the Cisco Unified IP Conference Station 7936, uses button 1 for line 1.
Standard 7935	The Standard 7935 template, which is not configurable for the Cisco IP Conference Station 7935, uses button 1 for line 1.
Standard 30 SP+	The Standard 30 SP+ template uses buttons 1 through 4 for lines, button 5 for call park, buttons 6 through 8 and 17 through 21 remain undefined, and buttons 9 through 13 and 22 through 25 apply for speed dial; button 14 applies for message-waiting indicator, button 15 for forward, and button 16 for conference. **Note** For only the Cisco IP Phone model 30 SP+, assign button 26 for automatic echo cancellation (AEC).

Table 43-2 Default Phone Button Templates Listed by Model (continued)

Phone Button Template Name	Template Description
Standard 30 VIP	The Standard 30 VIP template uses buttons 1 through 4 for lines, button 5 for call park, buttons 6 through 13 and 22 through 26 for speed dial, button 14 for message-waiting indicator, button 15 for call forward, and button 16 for conference.
Standard 12 Series, including the 12 S, 12 SP, and 12 SP+	The Standard 12 S, Standard 12 SP, and Standard 12 SP + templates use buttons 1 and 2 for lines, button 3 for redial, buttons 4 through 6 for speed dial, button 7 for hold, button 8 for transfer, button 9 for forwarding, button 10 for call park, button 11 for message waiting, and button 12 for conference.
Standard VGC Phone	The Standard VGC Phone template for the Cisco VG248 Gateway uses button 1 for a line and buttons 2 through 10 for speed dials.
Default VGC Virtual Phone	The Default VGC Virtual Phone template for the Cisco VGC Virtual Phone uses button 1 for line 1.
Standard ATA 186)	The Standard ATA 186 template uses button 1 for a line and buttons 2 through 10 for speed dials.
ISDN BRI Phone	The ISDN BRI Phone template uses button 1 for line 1.
Default IP Communicator	The Default IP Communicator template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys (by configuring the softkey template to the phone).
Standard IP-STE	The Standard IP-STE template uses buttons 1 and 2 for lines.
Standard Analog	The Standard Analog template for analog phones uses button 1 for line 1.
Third-Party SIP Device (Advanced)	The Generic SIP Phone - 2 Lines template, which is used for third-party SIP phones, uses buttons 1 and 2 for lines.
Third-Party SIP Device (Basic)	The Generic SIP Phone - 2 Lines template, which is used for third-party SIP phones, uses buttons 1 and 2 for lines.
StandardCN622	The StandardCN622 template, used for the Static SIP Mobile Subscriber, uses buttons 1 through 6 for lines.

Guidelines for Customizing Phone Button Templates

Use the following guidelines when you are creating custom phone button templates:

- Make sure that phone users receive a quick reference card or getting started guide that describes the most basic features of the custom template. If you create a custom template for employees in your company to use, make sure that it includes the following features and that you describe them on the quick reference card that you create for your users.
  - Cisco Unified IP Phone 7970/71, 7960/61, 7940/41, 7911—Line (one or more)
  - Cisco Unified IP Phone 7912—Line, speed dial, hold, and settings
  - Cisco Unified IP Phone 7910—Forward all
  - Cisco Unified IP Phone 7905 and 7902—Line, speed dial, hold, and settings

  - Cisco Wireless IP Phone 7920—Line (one or more)
  - Cisco IP Phone model 12 SP+—Line (one or more), hold, call park, and forward all
  - Cisco IP Phone model 30 VIP—Line (one or more), call park, and forward all
  - Cisco VGC Virtual Phone and Cisco ATA 186—Line and speed dials
- Consider the nature of each feature to determine how to configure your phone button template. You may want to assign multiple buttons to speed dial and line; however, you usually require only one of the other phone button features that are described in Table 43-3.

Table 43-3 Phone Button Feature Description

Feature	Description
AEC	If you are configuring a template for the Cisco IP Phone model 30 VIP, you must include one occurrence of this feature and assign it to button 26. Auto echo cancellation (AEC) reduces the amount of feedback that the called party receives when the calling party is using a speakerphone. Users should press the AEC button on a Cisco IP Phone model 30 SP+ when they are using speakerphone. Users do not need to press this button when speakerphone is not in use. This feature requires no configuration for it to work.
Answer/release	In conjunction with a headset apparatus, the user can press a button on the headset apparatus to answer and release (disconnect) calls.
Auto answer	If this feature is programmed on the template, pressing this button causes the speakerphone to go off hook automatically when an incoming call is received. **Note** You configure this feature for some phones models by using the Phone Button Template window and you configure this feature for some phone models by using the Phone Configuration window.
Call park	In conjunction with a call park number or range, when the user presses this button, call park places the call at a directory number for later retrieval. You must have a call park number or range that is configured in the system for this button to work, and you should provide that number or range to your users, so they can dial in to the number(s) to retrieve calls.
Conference	Users can initiate an ad hoc conference and add participants by pressing the Conference button. (Users can also use the Join softkey to initiate an ad hoc conference.) Only the person who initiates an ad hoc conference needs a conference button. You must make sure that an ad hoc conference bridge device is configured in Cisco Unified CallManager Administration for this button to work. Refer to the "Conference Bridges" chapter for more information.
Forward all	Users press this button to forward all calls to the designated directory number. Users can designate forward all in the Cisco Unified IP Phone Configuration windows, or you can designate a forward all number for each user in Cisco Unified CallManager Administration.

Table 43-3 Phone Button Feature Description (continued)

Feature	Description
Hold	Users press this button to place an active call on hold. To retrieve a call on hold, users press the flashing line button or lift the handset and press the flashing line button for the call on hold. The caller on hold receives a tone every 10 seconds to indicate the hold status or music (if the Music On Hold feature is configured). The hold tone feature requires no configuration to work.
Line	Users press this button to dial a number or to answer an incoming call. For this button to work, you must have added directory numbers on the user phone.
Meet-Me conference	When users press this button, they initiate a meet-me conference, and they expect other invited users to dial in to the conference. Only the person who initiates a meet-me conference needs a meet-me button. You must make sure that a meet-me conference device is configured in Cisco Unified CallManager Administration for this button to work.
Message waiting	Users press this button to connect to the voice-messaging system.
None	Use None to leave a button unassigned.
Redial	Users press this button to redial the last number that was dialed on the Cisco Unified IP Phone. This feature requires no configuration to work.
Privacy	Users press this button to activate/deactivate privacy.
Service URL	Users press this button to access a Cisco Unified IP Phone Service such as personal fast dials, stock quotes, or weather.
Speed-dial	Users press this button to speed dial a specified number. System administrators can designate speed-dial numbers in Cisco Unified CallManager Administration. Users can designate speed-dial numbers in the Cisco Unified IP Phone User Options Menu.
BLF/SpeedDial	Users monitor this button for the real-time status of the associated directory number or SIP URI on those devices that support the presence feature. Users press this button to dial the destination.
Transfer	Users press this button to transfer an active call to another directory number. This feature requires no configuration to work.

Softkey Templates

Use softkey templates to manage softkeys that are associated with applications such as Cisco Unified CM Assistant or call-processing features such as Cisco Call Back on the Cisco Unified IP Phones. The administrator uses the Softkey Template Configuration windows in Cisco Unified CallManager Administration to create and update softkey templates.

Cisco Unified CallManager supports two types of softkey templates: standard and nonstandard. Standard softkey templates in the Cisco Unified CallManager database contain the recommended selection and positioning of the softkeys for an application. Cisco Unified CallManager provides the following standard softkey templates:

- Standard User
- Standard Feature
- Standard Unified CM Assistant
- Standard Unified CM Assistant Shared Mode Manager

Note The default process does not assign a softkey template to the Cisco Unified IP Phone. The administrator must assign standard or nonstandard softkey templates to the Cisco Unified IP Phone by assigning the templates individually to each phone or by assigning the device pool to each phone.

The administrator creates a nonstandard softkey template by using the Softkey Template Configuration windows in Cisco Unified CallManager Administration. To create a nonstandard softkey template, the administrator copies a standard softkey template and makes changes. The administrator can add and remove applications that are associated with any nonstandard softkey template. Additionally, the administrator can configure softkey sets for each call state for a nonstandard softkey template.

The Softkey Template Configuration window lists the standard and nonstandard softkey templates and uses different icons to differentiate between standard and nonstandard templates.

The administrator assigns softkey templates in the following Cisco Unified CallManager Administration configuration windows:

- Device Pool Configuration
- Phone Configuration (SIP and SCCP)
- User Device Profile Configuration
- Default Device Profile Configuration

Add Application

The administrator can add a standard softkey template that is associated with a Cisco application to a nonstandard softkey template. When the administrator clicks the Add Application button from the Softkey Template Configuration window, a separate window displays and allows the administrator to choose the standard softkey template that is to be added to the end of the nonstandard softkey template. Duplicate softkeys get deleted from the end of the set that is moving to the front of the set.

Tip To refresh the softkeys for an application in the nonstandard softkey template, choose the standard softkey template that is already associated with the nonstandard softkey template. For example, if the administrator originally copied the Standard User template and deleted some buttons, choose the Standard User softkey template by clicking on the Add Application button. This adds the buttons that are included in the chosen softkey template.

The number of softkeys in any given call state cannot exceed 16. A message displays, and the add application procedure stops when the maximum number of softkeys is reached. The administrator must manually remove some softkeys from the call state before trying to add another application to the template.

The Delete Application button allows the administrator to delete application softkey templates that are associated with a nonstandard softkey template. Only the softkeys that are associated with the application get deleted. When softkeys are commonly shared between applications, they remain in the softkey template until the last application that shares the softkeys is removed from the softkey template.

Configure Softkey Layout

The administrator can configure softkey sets for each call state for a nonstandard softkey template. When the administrator chooses Configure Softkey Layout from the Related Links drop-down list box on the Softkey Template Configuration window and clicks **Go**, Softkey Layout Configuration displays.

The Softkey Layout Configuration pane contains the following fields:

- Call states—This drop-down list box displays the different call states of a Cisco Unified IP Phone. You cannot add, update, or delete call states. The call state that gets chosen from the drop-down list box indicates the softkeys that are available for that call state. Table 43-4 lists the call states.

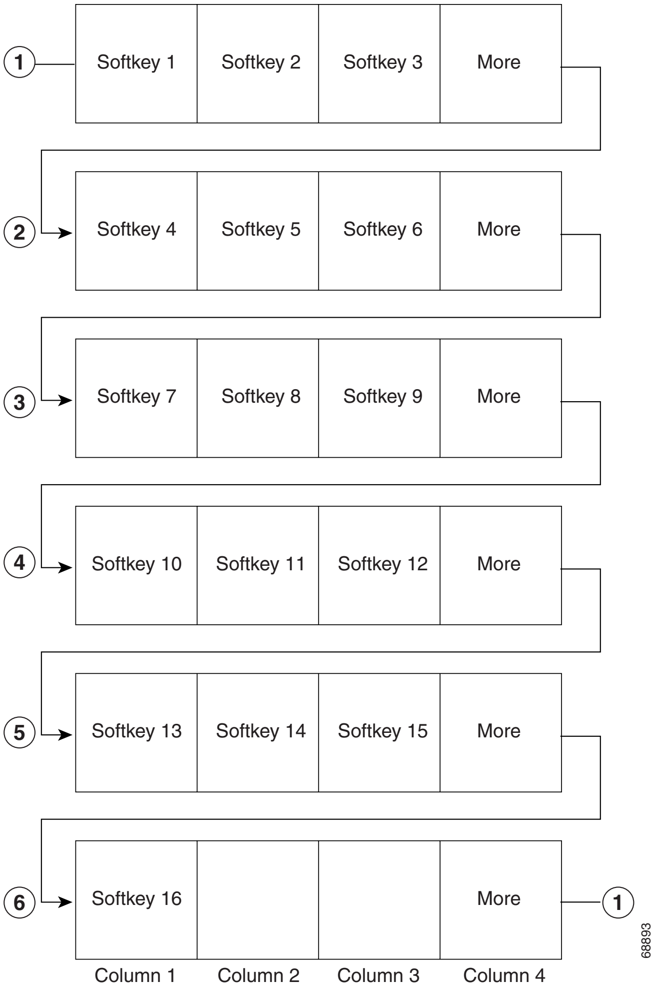
Table 43-4 Call States

Call State	Description
Connected	Displays when call is connected
Connected Conference	Consultation call for conference in connected call state
Connected Transfer	Consultation call for transfer in connected call state
Digits After First	Off-hook call state after user enters the first digit
Off Hook	Dial tone presented to phone
Off Hook With Feature	Off-hook call state for transfer or conference consultation call
On Hold	Call on hold
On Hook	No call exists for that phone.
Remote In Use	Another device that shares the same line uses call.
Ring In	Call received and ringing
Ring Out	Call initiated and the destination ringing

- Unselected Softkeys—Lists softkeys that are associated with a call state. This field lists the unselected, optional softkeys of the call state that displays in the Select a Call State to Configure drop-down list box. The softkeys that are listed in this field get added to the Selected Softkeys field by using the right arrows. You can add the Undefined softkey more than once to the Selected Softkey list. Choosing Undefined results in a blank softkey on the Cisco Unified IP Phone.
- Selected Softkeys—Lists softkeys that are associated with the chosen call state. This field lists the chosen softkeys of the call state that displays in the Select a Call State to Configure drop-down list box. The maximum number of softkeys in this field cannot exceed 16. See Figure 43-1 for a sample softkey layout.

Note Cisco recommends that a softkey remain in the same position for each call state. This provides the user with consistency and ease of use; for example, the More softkey always appears in the fourth softkey position from the left for each call state.

Figure 43-1 Sample Softkey Layout



Softkey Template Operation

For applications such as Cisco Unified CM Assistant to support softkeys, ensure softkeys and softkey sets are configured in the database for each device that uses the application.

You can mix application and call-processing softkeys in any softkey template. A static softkey template associates with a device in the database. When a device registers with Cisco Unified CallManager, the static softkey template gets read from the database into call processing and then gets passed to the device to be used throughout the session (until the device is no longer registered or is reset). When a device resets, it may get a different softkey template or softkey layout because of updates that the administrator makes.

Softkeys support a field called application ID. An application, such as Cisco Unified CM Assistant, activates/deactivates application softkeys by sending a request to the device through the Cisco CTIManager and call processing with a specific application ID.

When a user logs in to the Cisco IP Manager Assistant service and chooses an assistant for the service, the application sends a request to the device, through Cisco CTIManager and call processing, to activate all its softkeys with its application ID.

At any time, several softkey sets may display on a Cisco Unified IP Phone (one set of softkeys for each call).

The softkey template that is associated with a device (such as a Cisco Unified IP Phone) in the database designates the one that is used when the device registers with call processing. Perform the association of softkey templates and devices by using Softkey Template configuration in Cisco Unified CallManager Administration. See "Softkey Template Configuration" in the *Cisco Unified CallManager Administration Guide*.

Common Phone Profiles

Cisco Unified CallManager uses common phone profiles to define phone attributes that are associated with Cisco Unified IP Phones. Having these attributes in a profile instead of adding them individually to every phone decreases the amount of time that administrators spend configuring phones and allows the administrator to change the values for a group of phones. Common phone profiles specify the following attributes:

- Profile name
- Profile description
- Local phone unlock password
- End user access to phone background image setting

The common phone profile remains a required field when phones are configured; therefore, you must create the common phone profile before you create a phone. Cisco Unified CallManager provides a Standard Common Phone Profile that you can copy and modify to create a new common phone profile. You cannot, however, modify nor delete the Standard Common Phone Profile.

For information on configuring common phone profiles, see "Common Phone Profile Configuration" in the *Cisco Unified CallManager Administration Guide*.

Methods for Adding Phones

You can automatically add phones that support either the SCCP or SIP protocols to the Cisco Unified CallManager database by using autoregistration, manually by using the phone configuration windows, or in groups with the Bulk Administration Tool (BAT).

By enabling autoregistration before you begin installing phones, you can automatically add a Cisco Unified IP Phone to the Cisco Unified CallManager database when you connect the phone to your IP telephony network. For information on enabling autoregistration, refer to "Enabling Autoregistration" in the *Cisco Unified CallManager Administration Guide*. During autoregistration, Cisco Unified CallManager assigns the next available sequential directory number to the phone. In many cases, you may not want to use autoregistration; for example, if you want to assign a specific directory number to a phone or if you plan to implement authentication or encryption, as described in the *Cisco Unified CallManager Security Guide.*

Tip Cisco Unified CallManager automatically disables autoregistration if you configure the clusterwide security mode for authentication and encryption through the Cisco CTL client.

If you do not use autoregistration, you must manually add phones to the Cisco Unified CallManager database or use the Bulk Administration Tool (BAT). BAT enables system administrators to perform batch add, modify, and delete operations on large numbers of Cisco Unified IP Phones. Refer to the *Cisco Unified CallManager Bulk Administration Guide* for detailed instructions on using BAT.

User/Phone Add

You can use the End User, Phone, DN, and LA Configuration window to add a new phone at the same time that you add a new end user. You can associate a directory number (DN) and line appearance (LA) for the new end user by using the same window. To access the End User, Phone, DN, and LA Configuration window, choose the **User Management > User/Phone Add** menu option. See "User/Phone Add Configuration" in the *Cisco Unified CallManager Administration Guide* for configuration details.

Note The End User, Phone, DN, and LA Configuration window only allows addition of a new end user and a new phone. The window does not allow entry of existing end users or existing phones.

Phone Features

Cisco Unified CallManager enables you to configure the following phone features on Cisco Unified IP Phones: barge, privacy release, call back, call park, call pickup, immediate divert, malicious call identification, quality report tool, service URL, and speed dial and abbreviated dial.

For information about features that are related to directory numbers, see the "Directory Number Features" section on page 18-5. The following features get configured for directory numbers: call forward and call waiting.

Barge and Privacy

The Barge and Privacy features work together. Both features work with shared lines only.

Barge adds a user to a call that is in progress. Pressing the Barge of cBarge softkey automatically adds the user (initiator) to the shared line call (target), and the users currently on the call receive a tone. Barge supports built-in conference and shared conference bridges.

Privacy allows a user to allow or disallow other users of shared-line devices to view the device call information or to allow another user to barge in to its active calls.

For more information about Barge and Privacy, refer to Barge and Privacy in the *Cisco Unified CallManager Features and Services Guide*.

Call Forward

Call forward allows a user to configure a Cisco Unified IP Phone, so all calls that are destined for it ring another phone. The following types of call forward exist:

- Call forward all—Forwards all calls.
- Call forward busy—Forwards calls only when the line is in use and busy trigger setting is reached.
- Call forward no answer—Forwards calls when the phone is not answered after the configured no answer ring duration, or if the destination is unregistered.
- Call forward no coverage—Forward calls when either exhausts or times out, and the associated hunt-pilot for coverage specifies Use Personal Preferences for its final forwarding.

Each of these call forward types can be configured for internal and external calls and can be forwarded to voice mail or a dialed destination number by configuring the calling search space.

Cisco Unified CallManager includes the field, secondary Calling Search Space (CSS) for Call Forward All (CFA). The secondary CSS for CFA is combined with the existing CSS for CFA to allow the support of the alternate CSS system configuration. When CFA is activated, only the primary and secondary CSS for CFA is used to validate the CFA destination and redirect the call to the CFA destination. If these fields are empty, then the null CSS is used. Only the CSS fields configured in the primary CSS for CFA and secondary CSS for CFA fields are used. If CFA is activated from the phone, the CFA destination is validated using the CSS for CFA and the secondary CSS for CFA, and the CFA destination is written to the database. In previous releases, if the CSS for CFA is empty, the CFA destination got validated against the combination of the line CSS and device CSS of the phone. In this release, when activating the CFA, the CFA destination always gets validated against the CSS for CFA and the secondary CSS for CFA.

The administrator configures call forward information display options to the original dialed number or the redirected dialed number, or both. The administrator enables or disables the calling line ID (CLID) and calling name ID (CNID). The display option gets configured for each line appearance.

The call forward busy trigger gets configured for each line appearance in a cluster and cannot exceed the maximum number of calls that are configured for a line appearance. The call forward busy trigger determines how many active calls there are on a line before the call forward busy setting gets activated (for example, 10 calls).

The call forward no answer ring duration gets configured for each line appearance in a cluster, and the default specifies 12 seconds. The call forward no answer ring duration determines how long a phone rings before the call forward no answer setting gets activated.

Tip Keep the busy trigger slightly lower than the maximum number of calls, so that users have the ability to make outgoing calls and perform transfers.

Configure call forward in the Directory Number Configuration window in Cisco Unified CallManager Administration.

Call Park

Call park allows a user to place a call on hold, so anyone who is configured to use call park on the Cisco Unified CallManager system can retrieve it.

For example, if a user is on an active call at extension 1000, the user can park the call to a call park extension such as 1234, and another use can dial 1234 to retrieve the call.

To use call park, you must add the call park extension (in this case, 1234) in Cisco Unified CallManager Administration when you are configuring phone features. For more information about call park, refer to Call Park in the *Cisco Unified CallManager Features and Services Guide*.

Call Pickup

Cisco Unified CallManager provides the following types of call pickup:

- Call pickup—Allows you to answer a ringing phone in your designated call pickup group.
- Group call pickup—Allows you to answer incoming calls in another pickup group.
- Other group call pickup—Allows you to answer incoming calls in a pickup group that is associated with your own group.

All three types of call pickup can operate automatically or manually. If the service parameter, AutoCallPickupEnabled, is enabled, the Cisco Unified CallManager automatically connects you to the incoming call after you press one of the following softkeys on the phone:

- Pickup—For call pickup (calls in your own pickup group)
- GPickup—For group call pickup (calls in another pickup group)
- OPickup—For other group call pickup (calls in a pickup group that is associated with your own pickup group)

After the call pickup feature is automated, you need to use only one keystroke for a call connection except for group call pickup. You dial the DN of that other pickup group after you press the GPickup softkey on the phone.

Note CTI applications supports monitoring of the party whose call is picked up. CTI applications do not support monitoring of the pickup requester or the destination of the call that is picked up. Hence, Cisco Unified CM Assistant does not support auto call pickup (one-touch call pickup).

You configure the call pickup feature when you are configuring phone features in Cisco Unified CallManager.

When adding a line, you can indicate the call pickup group. The call pickup group indicates a number that can be dialed to answer calls to this directory number (in the specified partition). For more information about call pickup, refer to Call Pickup Group in the *Cisco Unified CallManager Features and Services Guide*.

Call Select

The Select softkey allows a user to select a call for feature activation, or to lock the call from other devices that share the same line appearance. Pressing the Select softkey on a selected call deselects the call.

When the call gets selected by a device, it gets put in the Remote-In-Use state on all other devices that share the line appearance. No one can select a call that is in the Remote-In-Use state. In other words, selecting a call instance will lock it from other devices that share the same line appearance.

A special display symbol identifies selected calls.

Conference List

The conference list feature provides a list of participant directory numbers that are in an ad hoc conference. The name of the participant displays if it is configured in Cisco Unified CallManager Administration.

Any participant can invoke the conference list feature on the phone and can view the participants. The conference controller can invoke the conference list feature and can view and remove any participant in the conference by using the Remove softkey.

Direct Transfer

Using the DirTrfr and Select softkeys, a user can transfer any two established calls to remove the calls from the IP phone. For more information about Direct Transfer, see the "Making and Receiving Multiple Calls Per Directory Number" section on page 18-7.

Onhook Call Transfer

The Call Transfer feature supports the onhook (hangup) action as a possible last step to complete a call transfer. You must set the Transfer On-hook Enabled service parameter, which enables onhook call transfer, to True for onhook call transfer to succeed. If the service parameter is set to False, the onhook action ends the secondary call to the third party.

In the existing implementation, if user B has an active call on a particular line (from user A) and user B has not reached the maximum number of calls on this line, the Cisco Unified IP Phone provides a Transfer softkey to user B. If user B presses the Transfer softkey (or Transfer button, if available) once, user B receives dial tone and can make a secondary call: user B dials the number of a third-party (user C). Cisco Unified CallManager provides a Transfer softkey to user B again. If user B presses the Transfer softkey again (or Transfer button, if available), the transfer operation completes.

With the onhook call transfer implementation, user B can hang up after dialing user C's number, and the transfer completes. Both the existing and new implementations work in the case of a blind transfer (user B disconnects before user C answers) and also in the case of a consult transfer (user B waits for user C to answer and announces the call from user A).

The previous implementation remains unchanged: user B can press the Transfer softkey twice to complete the transfer.

Immediate Divert

The Immediate Divert feature allows you to immediately divert a call to a voice-messaging system. Managers and assistants, or anyone who shares lines, use this feature. When the call gets diverted, the line becomes available to make or receive new calls.

Access the Immediate Divert feature by using the iDivert softkey. Configure this softkey by using the Softkey Template Configuration window of Cisco Unified CallManager Administration. The softkey template gets assigned to phones that are in the Cisco Unified CallManager system.

For more information about Immediate Divert, refer to Immediate Divert in the *Cisco Unified CallManager Features and Services Guide*.

Join

Using the Join softkey, a user can join up to 15 established calls (for a total of 16) to create a conference. For more information about Join, see the "Making and Receiving Multiple Calls Per Directory Number" section on page 18-7.

Malicious Call Identification (MCID)

The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives this type of call, the Cisco Unified 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.

For more information about MCID, refer to the "Malicious Call Identification" chapter in the *Cisco Unified CallManager Features and Services Guide*.

Quality Report Tool

The Quality Report Tool (QRT), a voice-quality and general problem-reporting tool for Cisco Unified IP Phones, allows users to easily and accurately report audio and other general problems with their IP phone. QRT gets loaded as part of the Cisco Unified CallManager installation, and the Cisco Extended Functions (CEF) service supports it.

As system administrator, you 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 level of user interaction that you want with QRT. You then define how the feature will work in your system by configuring system parameters and setting up Cisco Unified CallManager Serviceability tools. You can create, customize, and view phone problem reports by using the QRT Viewer application.

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
- Contains an internal HTTP server

Note For more information, refer to the following URL for the appropriate Cisco Unified IP Phone guide for your phone model:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm.

When users experience problems with their IP phones, they can report the type of problem and other relevant statistics by pressing the QRT softkey on the Cisco Unified 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, a user can then choose the reason code that best describes the problem that is being reported for the IP phone. A customized phone problem report provides you with the specific information.

For detailed information about configuring and using the Quality Report Tool feature, refer to Quality Report Tool in the *Cisco Unified CallManager Features and Services Guide*. For more information about configuring and using the QRT Viewer, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

For information about the user interface, refer to the appropriate Cisco Unified IP Phone Guide for your model IP phone and the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*.

Call Diagnostics and Voice-Quality Metrics

You can configure Cisco Unified IP Phones to collect call diagnostics and voice-quality metrics by setting a service parameter in Cisco Unified CallManager Administration as described in the following steps:

1. From Cisco Unified CallManager Administration, choose **System > Service Parameters**.
2. In Clusterwide Parameters (Device - General), locate the Call Diagnostics Enabled service parameter.
3. From the drop-down list box, choose one of the following states:

- Enabled Only When CDR Enabled Flag is True
- Enabled Regardless of CDR Enabled Flag

4. Click **Save**.

For more information about configuring service parameters in Cisco Unified CallManager Administration, refer to "Service Parameters Configuration" in the *Cisco Unified CallManager Administration Guide*. For information on configuring Cisco Unified IP Phones in

Cisco Unified CallManager Administration, refer to "Cisco Unified IP Phone Configuration" in the *Cisco Unified CallManager Administration Guide*. For information on configuring the Cisco Unified IP Phones for which call diagnostics and voice-quality metrics are available, refer to the Cisco Unified IP Phone user and administration documentation.

Service URL

You can also configure a Cisco Unified IP Phone Service URL, such as the extension mobility service, to a phone button. When the button gets pressed, the service gets invoked.

To configure a service URL on a phone button for the user, the administrator performs the following steps:

1. Using Cisco Unified IP Phone Services Configuration, create a service.
2. Using Phone Button Configuration, create a custom phone button template to include the service URL feature.
3. Using Phone Configuration, add the custom phone button template to each phone that requires the service URL button.
4. Using Phone Configuration, subscribe to each appropriate service.
5. Using Phone Configuration, add the service URL button.
6. Notify the users to configure services for their phone by using the Add/Update your Service URL Buttons link on the User Options Menu.

Speed Dial and Abbreviated Dial

Cisco Unified CallManager supports the configuration of up to 99 speed-dial entries, which are accessed through phone buttons and abbreviated dialing.

When the user configures up to 99 speed-dial entries, part of the speed-dial entries can be assigned to the speed-dial buttons on the IP phone; the remaining speed-dial entries are used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays, and the user can access any speed-dial entry by entering the appropriate index. For information about configuring speed dials, see "Configuring Speed-Dial Buttons" in the *Cisco Unified CallManager Administration Guide*.

Phone Association

Users can control some devices, such as phones. Applications that are identified as users control other devices, such as CTI ports. When users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding. For more information on associating phones with users, refer to the "Associating Devices to an End User" section in the *Cisco Unified CallManager Administration Guide*.

Phone Administration Tips

The following sections contain information that may help you configure phones in Cisco Unified CallManager Administration.

Phone Search

The following sections describe how to modify your search to locate a phone. If you have thousands of Cisco Unified IP Phones in your network, you may need to limit your search to find the phone that you want. If you are unable to locate a phone, you may need to expand your search to include more phones.

Note Be aware that the phone search is not case sensitive.

Searching by Device Name

When you enter the MAC address of the device in the MAC Address field when you are adding the phone, you can search by using that value as the Device Name in the Find and List Phones window.

Searching by Description

If you enter a user name and/or extension in the Description field when you are adding the phone, you can search by using that value in the Find and List Phones window.

Searching by Directory Number

To search for a phone by its directory number (DN), choose Directory Number. Choose a search criterion (such as begins with or ends with) and either choose a directory number from the drop-down list box below the **Find** button or enter a search string. Click the **Find** button to perform the search.

Note Some directory numbers do not associate with phones. To search for those directory numbers, which are called unassigned DN, use the Route Plan Report window or use the Directory Number Configuration Find/List window.

Searching by Calling Search Space

If you choose calling search space, the options that are available in the database display; you can choose one of these options from the drop-down list box below the **Find** button.

Searching by Device Pool

If you choose device pool, the options that are available in the database display (for example, Default); you can choose one of these options from the drop-down list box below the **Find** button.

Searching by Device Type

To search for a phone by its device type, choose Device Type and either enter a device type or choose a device type from the drop-down list box below the **Find** button.

Searching by Call Pickup Group

To search for a phone by its call pickup group, choose Call Pickup Group. If you choose Call Pickup Group, the options that are available in the database display; you can choose one of these options from the drop-down below the **Find** button. Alternatively, click the **Find** button only.

Searching by LSC Status

If you choose LSC status, the options that are available in the database display (for example, Operation Pending); you can choose one of these options from the drop-down list box below the **Find** button.

Searching by Authentication String

To search for a phone by an authentication string, choose Authentication String and enter an authentication string.

Searching by Device Protocol

To search for a phone by the protocol, choose Device Protocol and either enter a protocol, such as SIP, or choose a protocol from the drop-down list box below the **Find** button.

Searching by Security Profile

To search for a phone by its security profile, choose Security Profile and either enter a security profile name or choose a security profile from the drop-down list box below the **Find** button.

Search Within Results

To refine your search results, you can search for additional information. For example, if you search for phones by the device protocol, you may want to search within the device protocol results for phones that belong to a specific device pool. After you perform an initial search, check the Search Within Results check box. You can enter additional, or different, search criteria in the drop-down list boxes. Click **Find** again to search within the previous results.

Finding All Phones in the Database

To find all phones that are registered in the database, choose Device Name from the list of fields; choose "is not empty" from the list of patterns; then, click the Find button.

Note The list in the Find and List Phones window does not include analog phones and fax machines that are connected to gateways (such as a Cisco VG200). This list shows only phones that are configured in Cisco Unified CallManager Administration.

Messages Button

By performing the following actions, you can configure a voice-messaging access number for the messages button on Cisco Unified IP Phone models 7970, 7960, and 7940, so users can access the voice-messaging system by simply pressing the messages button:

1. Configure the voice-mail pilot number by choosing **Voice Mail > Voice Mail Pilot**.
2. Configure the voice-mail profile by choosing **Voice Mail > Voice Mail Profile**.
3. Choose the appropriate profile from the Voice Mail Profile field on the Directory Number Configuration window. By default, this field uses the default voice-mail profile that uses the default voice-mail pilot number configuration.

Note Typically, you can edit the default voice-mail pilot and default voice-mail profiles to configure voice-messaging service for your site.

For more information on configuring a voice-messaging service, refer to the "Voice Mail Connectivity to Cisco Unified CallManager" chapter.

Note For the Cisco IP Phone models 12 SP+ and 30 VIP, you can use phone button templates to configure a button with the message-waiting feature for access to a voice-messaging service.

Directories Button

The Cisco Unified IP Phone models 7970, 7960, and 7940 can display a directory of employee names and phone numbers. Although you access this directory from the directories button on the IP phone, you must configure it before users can access it. To use the corporate directory, you must enter users into a Lightweight Directory Access Protocol (LDAP) directory that is configured with Cisco Unified CallManager.

The URL Directories enterprise parameter defines the URL that points to the global directory for display on Cisco Unified IP Phone models 7970, 7960, and 7940. The XML device configuration file for the phone stores this URL.

Tip If you are using IP addresses rather than DNS for name resolution, make sure that the URL Directories enterprise parameter value uses the IP address of the server for the hostname.

If the phone URL was not updated correctly after the URL Directories enterprise parameter was changed, try stopping and restarting the Cisco TFTP service; then, reset the phone.

Cisco Unified CallManager User Options

Cisco Unified IP Phone users access Cisco Unified CallManager User Options through their web browser, so they can configure a variety of features on their phone. Some of the configurable features include user locale, user password, call forward, speed dial, and personal address book. By setting enterprise parameters as either True or False, administrators can configure which features are made available to users; for example, the administrator can set the Show Speed Dial Settings enterprise parameter to False, and users would not be able to configure speed dials on their phones.

For more information on how to access and use Cisco Unified CallManager User Options, refer to the phone guide for the specific Cisco Unified IP Phone.

Maximum Phone Fallback Queue Depth Service Parameter

The Cisco CallManager service uses the Maximum Phone Fallback Queue Depth service parameter to control the number of phones to queue on the higher priority Cisco Unified CallManager when that Cisco Unified CallManager is available for registration. The default specifies 10 phones per second. If a primary Cisco Unified CallManager were to fail, the phones will fail over to the secondary Cisco Unified CallManager. The failover process happens as fast as possible, using the priority queues to regulate the number of devices that are currently registering.

When the primary Cisco Unified CallManager recovers, the phones get returned to that Cisco Unified CallManager; however, you do not need to remove a phone from a working Cisco Unified CallManager, in this case the secondary, as fast as possible because the phone is on a working system. The queue depth gets monitored (using the Maximum Phone Fallback Queue Depth service parameter setting) to determine whether the phone that is requesting registration gets registered now or later. If the queue depth is greater than 10 (default), the phone stays where it is and tries later to register to the primary Cisco Unified CallManager.

In the Service Parameters Configuration window, you can modify the Maximum Phone Fallback Queue Depth service parameter. If the performance value is set too high (the maximum setting specifies 500), phone registrations could slow the Cisco Unified CallManager real-time response. If the value is set too low (the minimum setting specifies 1), the total time for a large group of phones to return to the primary Cisco Unified CallManager will be long.

Dependency Records

If you need to find out what directory numbers a specific phone is using or to what phones a directory number is assigned, choose Dependency Records from the Related Links drop-down list box on the Cisco Unified CallManager Administration Phone Configuration or Directory Number Configuration window. The Dependency Records Summary window displays information about directory numbers that are using the phone. To find out more information about the directory number, click the directory number, 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 the "Accessing Dependency Records" section and the "Removing a Directory Number from a Phone" section in the *Cisco Unified CallManager Administration Guide*.

Phone Failover and Fallback

This section describes how phones failover and fallback if the Cisco Unified CallManager to which they are registered becomes unreachable. This section also covers conditions that can affect calls that are associated with a phone, such as reset or restart.

Cisco Unified CallManager Fails or Becomes Unreachable

The active Cisco Unified CallManager designation applies to the Cisco Unified CallManager from which the phone receives call-processing services. The active Cisco Unified CallManager usually serves as the primary Cisco Unified CallManager for that phone (unless the primary is not available).

If the active Cisco Unified CallManager fails or becomes unreachable, the phone attempts to register with the next available Cisco Unified CallManager in the Cisco Unified CallManager Group that is specified for the device pool to which the phone belongs.

The phone device reregisters with the primary Cisco Unified CallManager as soon as it becomes available after a failure. See the "Maximum Phone Fallback Queue Depth Service Parameter" section on page 43-28 for information about phone registration during failover.

Note Phones do not failover or fallback while a call is in progress.

Phone is Reset

If a call is in progress, the phone does not reset until the call finishes.

Phone Configuration Checklist

Table 43-5 provides steps to manually configure an SCCP phone in Cisco Unified CallManager Administration. If you are using autoregistration, Cisco Unified CallManager adds the phone and automatically assigns the directory number.

Table 43-6 provides steps to manually configure a SIP phone in Cisco Unified CallManager Administration. If you are using autoregistration, Cisco Unified CallManager adds the phone and automatically assigns the directory number.

Table 43-5 Phone Configuration Checklist for SCCP Protocol

Configuration Steps		Procedures and Related Topics
Step 1	Gather the following information about the phone: • Model • MAC address • Physical location of the phone • Cisco Unified CallManager user to associate with the phone • Partition, calling search space, and location information, if used • Number of lines and associated DNs to assign to the phone	Phone Search, page 43-26
Step 2	Add and configure the phone.	Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 3	Add and configure lines (DNs) on the phone. You can also configure phone features such as call park, call forward, and call pickup.	Configuring a Directory Number, *Cisco Unified CallManager Administration Guide*
Step 4	Configure speed-dial buttons. You can configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the speed-dial settings on their phones by using Cisco Unified IP Phone User Options.	Configuring Speed-Dial Buttons, *Cisco Unified CallManager Administration Guide*
Step 5	Configure Cisco Unified IP Phone services. You can configure services for Cisco Unified IP Phone models 7970/71, 7960/61, 7940/41, 7912, and 7905 and Cisco IP Communicator if you want to provide services for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the services on their phones by using Cisco Unified CallManager User Options.	Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 6	Customize phone button templates and softkey templates, if required. Configure templates for each phone.	Configuring Phone Button Templates, *Cisco Unified CallManager Administration Guide* Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide* Adding Nonstandard Softkey Templates, *Cisco Unified CallManager Administration Guide*
Step 7	Configure the Busy Lamp Field feature, if required. You must use customized phone button templates to configure BLF/SpeedDial buttons.	BLF/SpeedDial Configuration Settings, *Cisco Unified CallManager Administration Guide*

Table 43-5 Phone Configuration Checklist for SCCP Protocol (continued)

Configuration Steps		Procedures and Related Topics
Step 8	Assign services to phone buttons, if required.	Adding a Cisco Unified IP Phone Service to a Phone Button, *Cisco Unified CallManager Administration Guide*
Step 9	Provide power, install, verify network connectivity, and configure network settings for the Cisco Unified IP Phone.	*Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*
Step 10	Associate user with the phone (if required).	Associating Devices to an End User, *Cisco Unified CallManager Administration Guide*
Step 11	Make calls with the Cisco Unified IP Phone.	Refer to the user guide for your Cisco Unified IP Phone.

Table 43-6 lists the configuration steps for Cisco Unified IP Phones that support SIP. For third-party SIP phones, see the Third-Party SIP Phone Configuration Checklist in the *Cisco Unified CallManager Administration Guide*.

Table 43-6 Phone Configuration Checklist for SIP Protocol

Configuration Steps		Procedures and Related Topics
Step 1	Gather the following information about the phone: • Model (7905, 7911, 7912, 7940, 7941, 7960, 7961, 7970, 7971) • MAC address • Physical location of the phone • Cisco Unified CallManager user to associate with the phone • Partition, calling search space, and location information, if used • Number of lines and associated DNs to assign to the phone	Phone Search, page 43-26
Step 2	If configuring the SIP phone in a secure mode, configure the SIP Phone Port on the Cisco Unified CallManager Configuration window.	Cisco Unified CallManager Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	If security is required, complete the SIP Security Profile Configuration. The SIP Security Profile gets added to the SIP phone by using the Phone Configuration window.	Phone Security Profile Configuration, *Cisco Unified CallManager Administration Guide* Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 4	Configure the SIP Profile. The SIP Profile gets added to the SIP phone by using the Phone Configuration window.	Configuring SIP Profiles, *Cisco Unified CallManager Administration Guide* Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*

Table 43-6 Phone Configuration Checklist for SIP Protocol (continued)

Configuration Steps		Procedures and Related Topics
Step 5	If you are using NTP for the timing synchronization, configure the NTP server by using the Phone NTP Reference Configuration window. Add the NTP server to Date/Time Group Configuration and then assign the date/time group to the device pool. Add the device pool to the SIP phone by using the Phone Configuration window.	Configuring the Phone NTP References, *Cisco Unified CallManager Administration Guide* Configuring a Date/Time Group, *Cisco Unified CallManager Administration Guide* Configuring a Device Pool, *Cisco Unified CallManager Administration Guide* Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 6	If you want the digits collected before sending them to Cisco Unified CallManager, configure a SIP Phone Dial plan. Add the SIP Dial Rule to the SIP phone by using Phone Configuration.	Configuring SIP Dial Rules, *Cisco Unified CallManager Administration Guide* Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 7	Add and configure the SIP phone.	Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 8	Add and configure lines (DNs) on the phone. You can also configure phone features such as call park, call forward, and call pickup.	Configuring a Directory Number, *Cisco Unified CallManager Administration Guide*
Step 9	Configure speed-dial buttons. You can configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the speed-dial settings on their phones by using Cisco Unified CallManager User Options.	Configuring Speed-Dial Buttons, *Cisco Unified CallManager Administration Guide*
Step 10	Configure Cisco Unified IP Phone services. You can configure services for Cisco Unified IP Phone models 7970/71, 7960/61, 7940/41, 7912, 7911, and 7905 and Cisco IP Communicator if you want to provide services for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the services on their phones by using the Cisco Unified CallManager User Options window.	Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*

Table 43-6 Phone Configuration Checklist for SIP Protocol (continued)

Configuration Steps		Procedures and Related Topics
Step 11	Customize phone button templates and softkey templates, if required. Configure templates for each phone.	Configuring Phone Button Templates, *Cisco Unified CallManager Administration Guide* Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide* Adding Nonstandard Softkey Templates, *Cisco Unified CallManager Administration Guide*
Step 12	Configure the Busy Lamp Field feature, if required. You must use customized phone button templates to configure BLF/SpeedDial buttons.	BLF/SpeedDial Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 13	Assign services to phone buttons, if required.	Adding a Cisco Unified IP Phone Service to a Phone Button, *Cisco Unified CallManager Administration Guide*
Step 14	Provide power, install, verify network connectivity, and configure network settings for the Cisco Unified IP Phone.	*Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*
Step 15	Associate user with the phone (if required).	Associating Devices to an End User, *Cisco Unified CallManager Administration Guide*
Step 16	Make calls with the Cisco SIP IP Phone.	Refer to the user guide for your Cisco SIP IP Phone.

Where to Find More Information

Related Topics

- Understanding Directory Numbers, page 18-1
- Voice Mail Connectivity to Cisco Unified CallManager, page 29-1
- Enabling Autoregistration, *Cisco Unified CallManager Administration Guide*
- Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
- Associating Devices to an End User, *Cisco Unified CallManager Administration Guide*
- User/Phone Add Configuration, *Cisco Unified CallManager Administration Guide*
- Phone Button Template Configuration, *Cisco Unified CallManager Administration Guide*
- Common Phone Profile Configuration, *Cisco Unified CallManager Administration Guide*
- Configuring SIP Dial Rules, *Cisco Unified CallManager Administration Guide*
- Configuring SIP Profiles, *Cisco Unified CallManager Administration Guide*
- Configuring the Phone NTP References, *Cisco Unified CallManager Administration Guide*
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
- Barge and Privacy, *Cisco Unified CallManager Features and Services Guide*

- Call Park, *Cisco Unified CallManager Features and Services Guide*
- Call Pickup Group, *Cisco Unified CallManager Features and Services Guide*
- Immediate Divert, *Cisco Unified CallManager Features and Services Guide*
- Quality Report Tool, *Cisco Unified CallManager Features and Services Guide*
- Presence, *Cisco Unified CallManager Features and Services Guide*

Additional Cisco Unified CallManager Documentation

- Phone administration documentation that supports your phone model and this version of Cisco Unified CallManager
- Cisco Unified IP Phone user documentation
- Firmware release notes for your phone model
- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Security Guide*
- *Cisco Unified CallManager Assistant User Guide*
- *Cisco IP Communicator Administration Guide*

Understanding Video Telephony

Cisco Unified CallManager supports video telephony and thus unifies the world of voice and video calls. Video endpoints use Cisco Unified CallManager call-handling features and access a unified voice and video solution for dialing and connecting video calls.

The Cisco Unified CallManager video telephony solution offers these features:

- Supports video and video-related features, such as far-end camera control (FECC)
- Supports multiple logical channels that are needed to allow the transmission of video streams
- Transmits midcall, media-related messages that are needed for video (that is, transmits commands or indications that are needed for video calls)
- Supports H.323, Skinny Client Control Protocol (SCCP), and Session Initiation Protocol (SIP)
- Enhances locations and regions to provide bandwidth management
- Provides serviceability information, such as Call Detail Records (CDRs), about video calls

This section covers the following topics:

- Introducing Video Telephony, page 44-1
- Video Telephony and Cisco Serviceability, page 44-10
- Video Telephony Configuration Checklist, page 44-12
- Where to Find More Information, page 44-13

Introducing Video Telephony

The following topics discuss the details of video telephony in the Cisco Unified CallManager environment:

- Video Calls, page 44-2
- Video Codecs, page 44-2
- Video Network, page 44-3
- H.323 Video, page 44-4
- Skinny Client Control Protocol Video, page 44-6
- Skinny Client Control Protocol Video Bridging, page 44-6
- SIP Video, page 44-7
- Bandwidth Management, page 44-7

- Phone Configuration for Video Calls, page 44-9
- Additional Configuration for Video Calls, page 44-9
- Conference Control for Video Conferencing, page 44-9

Video Calls

The typical video call includes two or three Real-Time Protocol (RTP) streams in each direction (that is, four or six streams). The call can include the following stream types:

- Audio (same codecs as a normal call with additional codecs G.722 and G.728)
- Video (H.261, H.263, and Cisco VT Camera wideband video codecs) at a different port
- Far-end camera control (FECC) (optional)

SIP video supports the following video calls by using the SIP Signaling Interface (SSI):

- SIP to SIP
- SIP to H.323
- SIP to SCCP
- SIP intercluster trunk

SIP video calls also provide media control functions for video conferencing.

Call control for video calls operates the same way as the call control that governs all other calls. Refer to the "Call Control" section on page 22-2 in the Media Resource Management chapter.

Video Codecs

Common video codecs include H.261, an older video codec, H.263, a newer codec that gets used to provide internet protocol (IP) video, and H.264, a high-quality codec. The system supports H.264 for calls that use the Skinny Client Control Protocol (SCCP), H.323, and SIP protocols on originating and terminating endpoints only. The system also supports Regions and locations.

H.261 and H.263 codecs exhibit the following parameters and typical values:

- Bit rates range from 64 kbps to a few mbps. These bit rates can exist in any multiple of 100 bps.
- Resolution:
  - One-quarter Common Interchange Format (QCIF) (Resolution equals 176x144.)
  - Common Interchange Format (CIF) (Resolution equals 352x288.)
  - 4CIF (Resolution equals 704x576.)
  - Sub QCIF (SQCIF) (Resolution equals 128x96.)
  - 16CIF (Resolution equals 1408x1152.)
  - Custom Picture Format
- Frame Rate: 15 frames per second (fps), 30 fps
- Annexes: D.1, D.2, F, I, J, K, L.4, L.8, N, P.5, T, U, N, U, W

The Cisco VT Camera wideband video codec, which is a fixed-bit-rate codec, runs on a PC that is linked to a phone. This codec enables the PC to associate with a call that the phone receives.
Cisco Unified CallManager currently supports intracluster Cisco VT Camera wideband video codec calls but not intercluster Cisco VT Camera wideband video codec calls.

Cisco Unified Video Advantage supports the Cisco VT Camera wideband video and H.263 codecs which can be used for intracluster and intercluster calls respectively. The support is based on correct configuration with related capabilities and regions. This support also applies to mid-call.

The bandwidth of video calls equals the sum of the audio bandwidth and the video bandwidth. The total bandwidth does not include overhead.

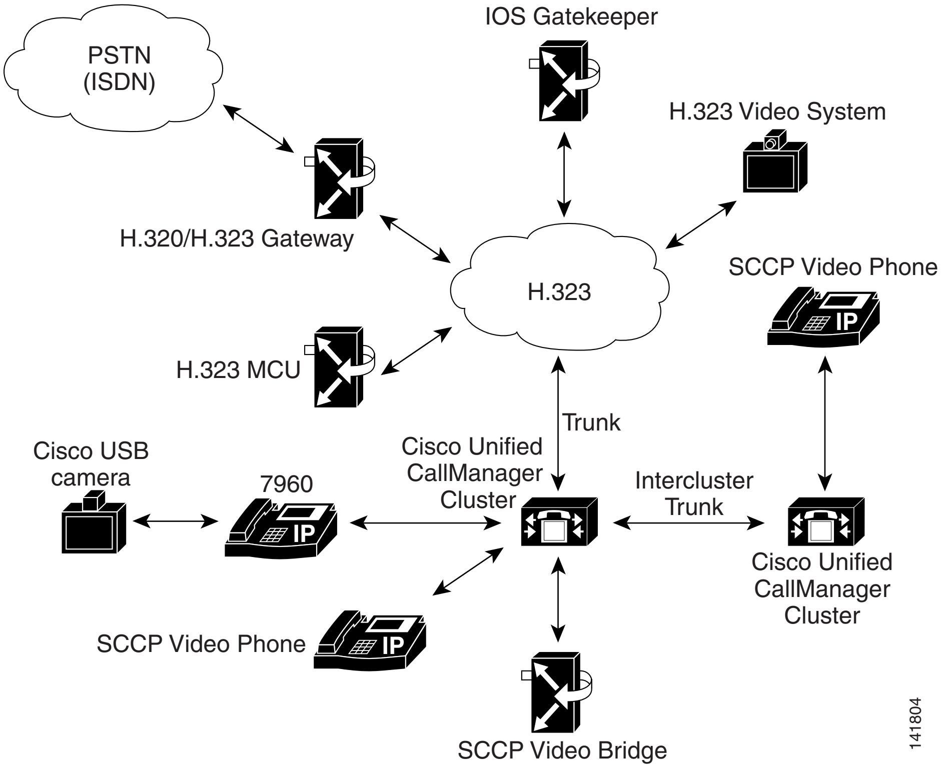
Example

A 384-kbps video call may be G.711 at 64 kbps (for audio) plus 320 kbps (for video). This sum does not include overhead. If the audio codec for a video call is G.729 (at 24 kbps), the video rate increases to maintain a total bandwidth of 384 kbps. If the call involves an H.323 endpoint, the H.323 endpoint may use less than the total video bandwidth that is available. Regardless of protocol, the endpoint may always choose to send at less than the max bit rate for the call.

Video Network

Figure 44-1 provides an example of a video network. In a successful video network, any endpoint can call any other endpoint. Video availability only exists if both endpoints are video enabled. Video capabilities extend across trunks.

Figure 44-1 Video Network Example



The Cisco video conference portfolio comprises the following H.323 devices:

- Cisco Unified Videoconferencing 3511 (Video Bridge or Media Control Unit [MCU])
- Cisco Unified Videoconferencing 3521 (BRI H.323/H.320 gateway)
- Cisco Unified Videoconferencing 3526 (PRI H.323/H.320 gateway)
- Cisco Unified Videoconferencing 3540 MCU (chassis-based bridge/gateway unit, which accepts multiple cards, and which supports H.323 and the Skinny Client Control Protocol. The IPVC Gateways only support H.323.)
- IOS H.323 Gatekeeper

Each of these devices supports the internet protocol (IP) network; the gateways support the Integrated Services Digital Network (ISDN).

Refer to the "Conference Bridge Configuration" section of the *Cisco Unified CallManager Administration Guide* for details of configuring the Cisco Unified Videoconferencing 3511 (MCU), 3540 (MCU) in Cisco Unified CallManager Administration.

Enabling an Audio-Only Device with Video

You can enable an audio-only device with video by using a Cisco application, Cisco Unified Video Advantage. You can associate the application with a Cisco Unified IP Phone. This association can occur before a call is made or during a call (mid-call). Cisco Unified IP Phones 7940/41, 7960/61, and 7970/71 support Cisco Unified Video Advantage.

For example, a call occurs from a Cisco Unified IP Phone 7960 to a video phone. The call is established as audio only. After Cisco Unified Video Advantage is associated with the Cisco Unified IP Phone 7960, the call gets reestablished as a video call.

During the association, Cisco Unified CallManager receives updated capabilities for the phone via existing SCCP messages. After the updated capabilities are received, Cisco Unified CallManager negotiates for video.

The media layer checks whether the regions allow video and whether both parties have video capabilities. If these conditions are met, the media layer establishes the video channels, and a video call gets established. Avoiding violation of administrative bandwidth constraints makes the region check necessary.

If the initial call involves an IP phone without a video, only audio location bandwidth gets reserved, and the media layer establishes an audio-only call.

H.323 Video

H.323 video exhibits the following characteristics:

- H.323 endpoints can be configured as H.323 phones, H.323 gateways, or H.323 trunks.
- Call forwarding, dial plan, and other call-routing-related features work with H.323 endpoints.
- H.323 video endpoints cannot initiate hold, resume, transfer, park, and other similar features.
- If an H.323 endpoint supports the empty capability set (ECS), the endpoint can be held, parked, and so forth.
- Some vendors implement call setup in such a way that they cannot increase the bandwidth of a call when the call gets transferred or redirected. In such cases, if the initial call is audio, users may not receive video when they are transferred to a video endpoint.

- No video media termination point (MTP) nor video transcoder currently exists. If an audio transcoder or MTP is inserted into a call, that call will be audio only. This is true when the IPVC audio transcoding capabilities is not being used. When the IPVC transcoders are used you can transcode the audio and send/receive video.
- For H.323 video calls, users must specify video call bandwidth.

Dynamic H.323 Addressing

You can configure a H.323 client with the E.164 address that is registered with the gatekeeper. E.164 addressing facilitates H.323 configuration and call routing by allowing the Cisco Unified CallManager to route all calls in place of the gatekeeper. The gatekeeper that is to be configured requires the following characteristics:

- Forward all calls to the Cisco Unified CallManager for routing.
- Calls that are routed from the Cisco Unified CallManager must not be routed back to the Cisco Unified CallManager.

Registering with the Gatekeeper

At boot time, Cisco Unified CallManager loads static configuration information such as the E.164 address and the configured gatekeeper for each H.323 client. The H.323 clients in the same gatekeeper zone stay in one group. A registration with the gatekeeper gets initiated for the group. The process does not require individual registration for each member of the group.

H.323 clients that belong to the same gatekeeper but different zone remain part of a different group, and only one registration is initiated for this group. H.323 devices that belong to a different gatekeeper zone remain part of another group, and only one registration is initiated for this group. All members of the same group use the same technology prefix.

Call Processing

During an outbound call where the H.323 client is the called party, Cisco Unified CallManager routes the call on the basis of DN to the H.323 device. Cisco Unified CallManager uses the H.323 device configuration to determine whether the gatekeeper is configured and sends an Admission Request Message (ARQ) with the configured E.164 address. If the device is registered with the gatekeeper, the gatekeeper sends an Admission Confirm Message (ACF) with the device's current IP address. Cisco Unified CallManager routes the call directly to this address.

During an inbound call where the H.323 device is the calling party, the gatekeeper routes the call to Cisco Unified CallManager. Cisco Unified CallManager uses the source E.164 address to determine whether the calling device is configured. Cisco Unified CallManager uses the configuration to determine the configuration for that phone. The phone configuration includes regions, locations, MRGL, etc.

Note the following items:

- The system does not support E.164 addressing on H.323 trunks, intercluster trunks and H.323 gateways.
- Cisco Unified CallManager does not resolve the device name when a gatekeeper-controlled H.323 client is configured. Cisco Unified CallManager can access the gatekeeper field for the H.323 client to discover the device. This enables Cisco Unified CallManager to bypass name resolution for the device name.

- Cisco Unified CallManager supports a maximum of one E.164 number per gatekeeper-controlled H.323 client. If the gatekeeper field is populated, you cannot configure a second DN. If an H.323 client is configured for more than one DN, you cannot add the extra gatekeeper information to the database.
- The Gatekeeper routes call by using zone information when there is no zone prefix.

Configuration Notes

Note the following items for configuration purposes:

- You must ensure that gatekeeper is configured in Cisco Unified CallManager before an H.323 client can specify that gatekeeper in its configuration. The Gatekeeper field stays empty by default.
- Ensure that the Gatekeeper field on H.323 client configuration is configured as it is for H.323 trunk.
- Be sure to add the gatekeeper name, technology prefix, zone, and E.164 fields to the H.323 client configuration. You do not need to add Terminal Type. Default specifies the gateway type. If the gatekeeper is not chosen for the gatekeeper field during configuration of each of these fields, these fields cannot populate.
- Gatekeeper, zone, technology prefix fields, and E.164 information display under H.323 Information group on H.323 Client configuration.
- When an H.323 client uses the same gatekeeper, zone and technology prefix as those of another client, consider both clients in the same group. This group represents a single endpoint to the gatekeeper.
- You cannot use the same zone name for the H.323 client and trunk. A zone that a H.323 client uses must differ from the one that an H.323 trunk or a gatekeeper-controlled intercluster trunk uses.
- Ensure the service parameter, Send Product Id and Version ID, is set to True.

If an H.323 client is configured with an E.164 address and a gatekeeper, the database stores this information when the configuration is updated. This information gets loaded at boot time or when the device is reset.

Skinny Client Control Protocol Video

Skinny Client Control Protocol video exhibits the following characteristics:

- If a Skinny Client Control Protocol phone reports video capabilities, Cisco Unified CallManager automatically opens a video channel if the other end supports video.
- For Skinny Client Control Protocol video calls, system administration determines video call bandwidth by using regions. The system does not ask users for bit rate.

Skinny Client Control Protocol Video Bridging

Video conferencing requires a Skinny Client Control Protocol video bridge. Skinny Client Control Protocol video bridging exhibits the following characteristics:

- Skinny Client Control Protocol video bridging requires the same setup as an audio bridge.
- Skinny Client Control Protocol video bridging supports a mix of audio and video in a conference.

- Media resource group lists determine whether an endpoint receives an audio or video bridge. That is, the media resource group list configuration of the user who sets up the conference determines whether the conference is a video conference or an audio-only conference. Refer to the "Media Resource Group List Configuration" section for details of configuring a media resource group list.

SIP Video

Cisco Unified CallManager video supports the SIP protocol, and both SIP trunks and lines support video signaling. SIP supports the H.261, H.263, and H.264 video codecs (it does not support the wideband video codec that is used by the VTA).

The following table lists the type of codes that SIP interfaces support.

Codec	RTP Payload Type
G.711 u-Law	0
GSM	3 (also referred to as GSM Full Rate)
G.723	4
G.711 a-Law	8
G.722	9
G.728	15
G.729	18 (support for combinations of AnnexA and AnnexB)

The Media Termination Point (MTP), which is used for RFC 2833, supports multiple logical channels within a session. A logical channel could be for audio or video. To support video channels, the MTP uses pass-through mode. Video pass-through is enabled if the MTP supports both pass-through and multiple logical channels. Not all MTP devices support multiple logical channels and pass-through mode.

Configuring a SIP Trunk for Video Calls

Perform the following steps to enable video calls on a SIP trunk:

- On the Trunk Configuration window in Cisco Unified CallManager Administration, check the Retry Video Call as Audio check box if you want the call to use audio when the video connection is not available.
- Reset the trunk.

For more information, see the "Additional Configuration for Video Calls" section on page 44-9 and the "Trunk Interaction with H.323 Client" section on page 44-9.

Bandwidth Management

Bandwidth management for video calls gets managed through the call admission control that regions and locations provide in Cisco Unified CallManager Administration.

Regions

Regions in Cisco Unified CallManager allow the bandwidth of video calls to be set. Video call bandwidth, which is the sum of the video bandwidth and the audio bandwidth, does not include overhead.

Refer to the "Region Configuration" section of the *Cisco Unified CallManager Administration Guide* for details of configuring regions in Cisco Unified CallManager.

Locations

Locations in Cisco Unified CallManager Administration include two pools, one pool for video calls and a separate pool for audio calls.

Refer to the "Location Configuration" section of the *Cisco Unified CallManager Administration Guide* for details of configuring locations in Cisco Unified CallManager.

RSVP

RSVP supports SCCP and SIP video calls. The RSVP policy for call admission control is configured by using the Location Configuration window in Cisco Unified CallManager Administration. For more information on the RSVP functionality, see the "Resource Reservation Protocol" section on page 9-1.

Alternate Routing

If an endpoint cannot obtain the bandwidth that it needs for a video call, a video call retries as an audio call for the default behavior. To use route/hunt lists or Automated Alternate Routing (AAR) groups to try different paths for such video calls, uncheck the Retry Video Call as Audio setting in the configuration settings for applicable gateways, trunks, and phones. Refer to the "Route List Configuration" and "Automated Alternate Routing Group Configuration" sections of the *Cisco Unified CallManager Administration Guide* for details.

DSCP Marking

Differentiated Services Code Point (DSCP) packet marking, which is used to specify the class of service for each packet, includes the following characteristics:

- Audio streams in audio-only calls default to EF.
- Video streams and associated audio streams in video calls default to AF41.
- You can change these defaults through the use of a service parameter. The following service parameter settings affect DSCP packet marking:
  - DSCP For Audio Calls (for media [RTP] streams)
  - DSCP For Video Calls (for media [RTP] streams)
  - DSCP for Audio Calls When RSVP Fails
  - DSCP for Video Calls when RSVP Fails
  - DSCP for ICCP Protocol Links

Phone Configuration for Video Calls

The following setting for video-enabled devices affects video calls:

- Retry Video Call as Audio—By default, this check box remains checked. Thus, if an endpoint (phone, gateway, trunk) cannot obtain the bandwidth that it needs for a video call, call control retries the call as an audio call. This setting applies to the destination devices of video calls.
- Video Capabilities Enabled/disabled—This drop-down list box turns video capabilities on and off.

Additional Configuration for Video Calls

The following configuration considerations also affect the ability to make video calls in Cisco Unified CallManager:

- Trunk interaction with the H.323 client
- Call routing considerations
- Resetting gateway timer parameters

Trunk Interaction with H.323 Client

Trunk interaction with the H.323 Client for video calls functions identically to interaction functions for audio calls. Refer to the "Trunks and Gatekeepers in Cisco Unified CallManager" section on page 42-2 in the Understanding Cisco Unified CallManager Trunk Types chapter.

Call Routing for Video Calls

Call routing for video calls functions identically to call routing for audio calls.

Gateway Timer Parameter

For some bonding calls through the H.323/H.320 gateway, the gateway requires a longer time to exchange the H.323 TCS message. If the time required is greater than the timer setting for several Cisco CallManager service parameters, Cisco Unified CallManager will drop the call.

If the default Cisco Unified CallManager gateway timer values appears to be too short, Cisco Unified CallManager drops the call before completion of the call connection. Cisco recommends increasing the following service parameter timers values to avoid call failure.

- H245TCSTimeout=25
- Media Exchange Interface CapabilityTimer=25
- Media Exchange Timer=25

Conference Control for Video Conferencing

Cisco Unified CallManager supports the following conference controls capabilities:

- Roster/Attendee List
- Drop Participant

- Terminate Conference
- Show Conference Chairperson/Controller
- Continuous Presence

Cisco Unified CallManager also supports the following video conference capabilities for Skinny Client Control Protocol phones:

- Display controls for video conferences. The Skinny Client Control Protocol phones can choose to use the continuous presence or voice-activated mode to view the video conference. When a mode is chosen, a message gets sent to the bridge to indicate which mode to use on the video channel. Switching between modes does not require renegotiation of media.
- Display participant information such as the user name in the video stream. The system can use the participant information for other conferencing features such as roster.

Video Telephony and Cisco Serviceability

Cisco Serviceability tracks video calls and conferences by updating performance monitoring counters, video bridge counters, and call detail records (CDRs).

Performance Monitoring Counters

Video telephony events cause updates to the following Cisco Unified CallManager Serviceability performance monitoring counters:

- Cisco Unified CallManager
  - VideoCallsActive
  - VideoCallsCompleted
  - VideoOutOfResources
- Cisco H.323
  - VideoCallsActive
  - VideoCallsCompleted
- Cisco Locations
  - VideoBandwidthAvailable
  - VideoBandwidthMaximum
  - VideoOutOfResources
  - VideoCurrentAvailableBandwidth
- Cisco Gatekeeper
  - VideoOutOfResources
- Cisco SIP
  - VideoCallsCompleted
  - VideoCallsActive

Refer to the *Cisco Unified CallManager Serviceability System Guide* and *Cisco Unified CallManager Serviceability Administration Guide* for details.

Video Bridge Counters

Video conference events cause updates to these Cisco video conference bridge performance monitoring counters:

- ConferencesActive
- ConferencesAvailable
- ConferencesCompleted
- ConferencesTotal
- OutOfConferences
- OutOfResources
- ResourceActive
- ResourceAvailable
- ResourceTotal

These counters also display in the Cisco Unified CallManager object with the VCB prefix.

Refer to the *Cisco Unified CallManager Serviceability System Guide* and *Cisco Unified CallManager Serviceability Administration Guide* for details

Call Detail Records

Video telephony events cause updates to Call Detail Records (CDRs) in Cisco Unified CallManager Serviceability. These CDRs include the following information:

- IP address and port for video channels
- Codec: H.261, H.263, H.264, Cisco VT Camera wideband video
- Call bandwidth
- Resolution: QCIF, CIF, SQCIF, 4CIF, 16CIF, or Custom Picture Format

Cisco Unified CallManager also stores CDRs for mid-call video and supports the following call scenarios:

- Skinny Client Control Protocol to Skinny Client Control Protocol calls
- Skinny Client Control Protocol to Skinny Client Control Protocol calls across an intercluster trunk (ICT)

Note CDR is added when video is added mid-call, but CDR entry is not removed as part of mid-call video removal (for example, Cisco Video Telephony Advantage gets turned off).

Refer to the *Cisco Unified CallManager Serviceability System Guide* and *Cisco Unified CallManager Serviceability Administration Guide* for details.

Video Telephony Configuration Checklist

Table 44-1 provides a checklist to configure video telephony in Cisco Unified CallManager Administration.

Table 44-1 Video Telephony Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	If you use regions for call admission control, configure regions for video call bandwidth. **Note** All devices have a default region, which defaults to 384 kbps for video.	Region Configuration, *Cisco Unified CallManager Administration Guide* Call Admission Control, *Cisco Unified CallManager System Guide*
Step 2	If you use locations for call admission control, configure locations for video call bandwidth.	Configuring a Location, *Cisco Unified CallManager Administration Guide* Call Admission Control, *Cisco Unified CallManager System Guide*
Step 3	If using RSVP for bandwidth management of SIP video calls, configure the RSVP service parameters, or set the RSVP policy in the Location Configuration window.	Configuring a Location, *Cisco Unified CallManager Administration Guide* Configuring Service Parameters for a Service on a Server, *Cisco Unified CallManager Administration Guide*
Step 4	To use a Cisco video conference bridge, configure the appropriate conference bridge for your network.	Conference Bridge Configuration, *Cisco Unified CallManager Administration Guide*
Step 5	To configure a user to use the video conference bridge instead of using other conference bridges, configure the user's media resource groups and media resource group lists accordingly.	Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide* Media Resource Group List Configuration, *Cisco Unified CallManager Administration Guide*
Step 6	Configure the H.323 gateways in your system to retry video calls as audio calls (default behavior) or configure AAR groups and route/hunt lists to use alternate routing for video calls that do not connect.	Gateway Configuration, *Cisco Unified CallManager Administration Guide* Automated Alternate Routing Group Configuration, *Cisco Unified CallManager Administration Guide* Route List Configuration, *Cisco Unified CallManager Administration Guide*

Table 44-1 Video Telephony Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 7	Configure the H.323 phones in your system to retry video calls as audio calls (default behavior) or configure AAR groups and route/hunt lists to use alternate routing for video calls that do not connect. Choose Enabled for Video Capabilities.	Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide* Automated Alternate Routing Group Configuration, *Cisco Unified CallManager Administration Guide* Route List Configuration, *Cisco Unified CallManager Administration Guide*
Step 8	Configure the H.323 trunks in your system to retry video calls as audio calls (default behavior) or configure AAR groups and route/hunt lists to use alternate routing for video calls that do not connect.	Trunk Configuration, *Cisco Unified CallManager Administration Guide* Automated Alternate Routing Group Configuration, *Cisco Unified CallManager Administration Guide* Route List Configuration, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topics

- Call Admission Control, *Cisco Unified CallManager System Guide*
- Region Configuration, *Cisco Unified CallManager Administration Guide*
- Location Configuration, *Cisco Unified CallManager Administration Guide*
- Conference Bridge Configuration, *Cisco Unified CallManager Administration Guide*
- Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide*
- Media Resource Group List Configuration, *Cisco Unified CallManager Administration Guide*
- Automated Alternate Routing Group Configuration, *Cisco Unified CallManager Administration Guide*
- Route List Configuration, *Cisco Unified CallManager Administration Guide*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*
- Trunk Configuration, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- Cisco Unified IP Phone administration documentation and release notes (all models)
- Cisco Unified IP Phone user documentation and release notes (all models)
- *Cisco Unified CallManager Serviceability System Guide*

- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified Videoconferencing 3511 MCU and Cisco Unified Videoconferencing 3540 MCU Module Administrator Guide*

CHAPTER 45

Computer Telephony Integration

Computer telephony integration (CTI) enables you to leverage computer-processing functions while making, receiving, and managing telephone calls. CTI applications allow you to perform such tasks as retrieving customer information from a database on the basis of information that caller ID provides. CTI applications can also enable you to use information that an interactive voice response (IVR) system captures, so the call can be routed to the appropriate customer service representative or so the information is provided to the individual who is receiving the call.

This section covers the following topics:

- Computer Telephony Integration Applications, page 45-1
- CTIManager, page 45-2
- CTI-Controlled Devices, page 45-3
- User Management and CTI Controlled Devices, page 45-5
- Applications That Monitor and Control All CTI-Controllable Devices, page 45-5
- Dependency Records, page 45-6
- CTI Redundancy, page 45-6
- CTI Configuration Checklist, page 45-8
- Where to Find More Information, page 45-9

Computer Telephony Integration Applications

The following list contains descriptions of some Cisco CTI applications that are available:

- Cisco IP Communicator—Cisco IP Communicator, a desktop application, turns your computer into a full-feature telephone with the added advantages of call tracking, desktop collaboration, and one-click dialing from online directories. You can also use Cisco IP Communicator in tandem with a Cisco Unified IP Phone to place, receive, and control calls from your desktop PC. All features function in both modes of operation.
- Cisco Unified CallManager AutoAttendant—The Cisco IP AutoAttendant application works with Cisco Unified CallManager to receive calls on specific telephone extensions and to allow the caller to choose an appropriate extension.
- Cisco Unified CallManager Attendant Console—This application provides a graphical user interface for controlling a Cisco Unified IP Phone to perform attendant console functions.

- Cisco WebDialer—Cisco WebDialer, which is installed on a Cisco Unified CallManager server and is used in conjunction with Cisco Unified CallManager, allows Cisco Unified IP Phone users to make calls from web and desktop applications.

Note To determine which Cisco Unified CallManager CTI applications support Cisco SIP IP phones, refer to the application-specific documentation.

CTIManager

A program called CTIManager includes the CTI components that interface with the applications that are separated out of Cisco Unified CallManager. The CTIManager service communicates with Cisco Unified CallManager by using the Cisco Unified CallManager communication framework, System Distribution Layer (SDL). Installation of the CTIManager program occurs on the Cisco Unified CallManager server during the Cisco Unified CallManager installation. You can have one or more CTIManagers active in a cluster, but only one CTIManager can exist on an individual server. An application (JTAPI/TAPI) can have simultaneous connections to multiple CTIManagers; however, an application can use only one connection at a time to open a device with media termination.

With CTIManager, applications can access resources and functionality of all Cisco Unified CallManagers in the cluster and have access to failover capability. When a CTIManager fails, the application can access the secondary CTIManager only if the application supports it (for JTAPI applications) or if the Cisco TAPI Service Provider (Cisco TSP) is properly configured (for TAPI applications). For more information about failover and fallback, see the “CTI Redundancy” section on page 45-6.

CTIManager provides two advanced, clusterwide service parameters that are used in conjunction with the CTI Super Provider capability:

- Maximum Devices Per Provider—This parameter specifies the maximum number of devices that a single CTI application can open. The default specifies 2000 devices.
- Maximum Devices Per Node—This parameter specifies the maximum number of devices that all CTI applications can open on any CTIManager node in the Cisco Unified CallManager system. The default specifies 800 devices.

If the configured limits are exceeded, CTI generates alarms, but the applications continue to operate with the extra devices. For more information on CTI Super Provider, see the “User Management and CTI Controlled Devices” section on page 45-5.

Media Termination Points

CTI applications can terminate media on CTI ports and CTI route points in the following ways:

- Static IP address and port number—Specify the media IP address and port number when the device gets opened. In this case, the media always terminates at the same IP address and port for all calls that are on that device. Only one application can terminate the media in this way.
- Dynamic IP address or port number—Specify the media IP address or port number on a per-call basis. For each call that requires a media termination, notification gets sent to the application that requests the media termination information. The application then must send the IP address or port number back, so the media can go through. You can specify only the IP address or port number on

a per-call basis. The capabilities of the device still get specified statically when the device is opened. With dynamic media termination, multiple applications can open a device (CTI port or route point) for media termination as long as the capabilities that each application specifies stay the same.

CTI-Controlled Devices

The following CTI-controlled device types exist:

- Cisco Unified IP Phones (SCCP and SIP)

Note CTI applications support only some Cisco SIP IP phones; for example, the Cisco SIP IP Phone 7940 and 7960 are not supported.

- CTI ports
- CTI route points

Cisco Unified IP Phones

CTI-controlled Cisco Unified IP Phones comprise SCCP phones that a CTI application can control. CTI supports Cisco SIP IP Phones (models 7911, 7941, 7961, 7970, and 7971) from the CTI interfaces JTAPI and TAPI, with some limited functionality. CTI applications control and monitor SIP phones in the same manner as CTI controlled/monitored SCCP phones.

For SCCP phones, outbound dialing supports enbloc (the phone collects all digits before passing them to Cisco Unified CallManager for routing) or digit-by-digit collection. If dialing is done digit-by-digit, a CTI dialing call state notification gets sent to the phone when it goes off hook and the first digit is pressed for an outgoing call. For enbloc outbound dialing, the dialing call state notification gets delayed until the phone collects all the digits and sends them to Cisco Unified CallManager for routing.

For SIP phones, enbloc dialing always gets used even if the user first goes off hook before dialing digits; the phone will wait until all the digits are collected before sending the digits to Cisco Unified CallManager. This means that the dialing call state notification will only get generated after enough digits are pressed on the phone to match one of the configured dialing patterns. In all cases, the dialing state notifications will always get generated prior to the call being routed to the destination (as is the case with SCCP phones).

SIP phones control when and how long to play reorder tone. When a SIP phone receives a request to play reorder tone, it releases the resources from Cisco Unified CallManager and plays reorder tone. Therefore, the call appears to be idle to a CTI application regardless of when reorder tone is played on the phone. In these scenarios, applications can receive and initiate calls from the phone whether there is reorder tone being played by the phone. Because resources have been released on Cisco Unified CallManager, the call does not count against the busy trigger and maximum number of call counters (that are configured on the Directory Number Configuration window).

Note Cisco SIP IP phones that are configured to use UDP as the transport mode (instead of TCP) will not support the device data pass-through functionality; for example, the Quality Reporting Tool (QRT) requires the data pass-through functionality, so it cannot be used with IP phones configured with UDP.

CTI Ports

CTI ports as virtual devices can have one or more virtual lines, and software-based Cisco Unified CallManager applications such as Cisco SoftPhone, Cisco Unified CallManager AutoAttendant, and Cisco Unified IP Interactive Voice Response (IVR) use them. You configure CTI ports by using the same Cisco Unified CallManager Administration windows as you use to configure phones. For first-party call control, you must add a CTI port for each active voice line.

CTI Route Point

A CTI route point virtual device can receive multiple, simultaneous calls for application-controlled redirection. You can configure one or more lines on a CTI route point that users can call to access the application. Applications can answer calls at a route point and can also redirect calls to a CTI port or IP phone. Route points can receive multiple, simultaneous calls; therefore, applications wanting to terminate media for calls at route points must specify the media and port for the call on a per-call basis.

CTI route points support the following features:

- Answer a call
- Make and receive multiple active calls
- Redirect a call
- Hold a call
- Unhold a call
- Drop a call

When a call arrives at a route point, the application must handle (accept, answer, redirect) it within a specified time. To configure the time that is allowed to answer a call, use the Cisco Unified CallManager CTI New Call Accept Timer service parameter. Use the Directory Number Configuration window in Cisco Unified CallManager Administration to configure the number of simultaneous active calls on the route point.

Note If you are planning to use a TAPI application to control CTI port devices by using the Cisco Unified CallManager Telephony Service Provider (TSP), you may only configure one line per CTI port device.

Applications that are identified as users can control CTI devices. When users have control of a device, they can control certain settings for that device, such as answer the call and call forwarding.

CTI devices (CTI ports, CTI route points) must associate with device pools that contain the list of eligible Cisco Unified CallManagers for those devices. For general instructions on how to configure settings for CTI ports, refer to the "Configuring Cisco Unified IP Phones" section in the *Cisco Unified CallManager Administration Guide*. For general instructions on how to configure settings for CTI route points, refer to the "Configuring a CTI Route Point" section in the *Cisco Unified CallManager Administration Guide*. For information on how to configure CTI ports and route points for use with a specific application, such as Cisco IP Communicator, refer to the documentation and online help that is provided with that application.

When a CTI device fails (during a Cisco Unified CallManager failure, for example), Cisco Unified CallManager maintains media streams that are already connected between devices (for devices that support this feature). Cisco Unified CallManager drops calls that are in the process of being set up or modified (transfer, conference, redirect, and so on).

User Management and CTI Controlled Devices

To allow a CTI application to control or monitor devices, the devices must be assigned to the end user or application user that is associated with the CTI application. This gets done by using the End User or Application User Configuration windows in Cisco Unified CallManager Administration. From the Device Association pane of the User Configuration window, an administrator associates the desired devices to the Controlled Devices list.

To allow CTI applications access to certain CTI capabilities, the end user or application user that is associated with the application must be added to one or more of the following CTI-related user groups:

- Standard CTI Allow Call Park Monitoring—This user group allows an application to receive notification when calls are parked/unparked to all Call Park directory numbers.
- Standard CTI Allow Calling Number Modification—This user group allows an application to modify the calling party number in supported CTI applications.
- Standard CTI Allow Control of All Devices—This user group allows an application to control or monitor any CTI-controllable device in the system.
- Standard CTI Allow Reception of SRTP Key Material—This user group allows an application to receive information that is necessary to decrypt encrypted media streams. This group typically gets used for recording and monitoring purposes.
- Standard CTI Enabled—This user group, which is required for all CTI applications, allows an application to connect to Cisco Unified CallManager to access CTI functionality.
- Standard CTI Secure Connection—Inclusion into this group will require that the application have a secure (TLS) CTI connection to Cisco Unified CallManager if the Cisco Unified CallManager cluster security is enabled.

Note The CTI application must support the specified user group to which it gets assigned. Refer to the appropriate application documentation for more information.

For more information on End User and User Group Configuration, see Adding an End User and Adding Users to a User Group in the *Cisco Unified CallManager Administration Guide*.

Note Cisco recommends that users associated with the Standard CTI Allow Control of All Devices user group also be associated with the Standard CTI Secure Connection user group.

Applications That Monitor and Control All CTI-Controllable Devices

By adding an application user to the user group, Standard CTI Allow Control of All Devices, a CTI application can control any CTI-controllable devices that are configured in the Cisco Unified CallManager system. These applications sometimes get referred to as super provider applications. CTI super provider application dynamically associates/disassociates devices to/from an application control list, so this list/set of devices could be a variable list/set. For example, if 10,000 CTI-controllable devices exist in a Cisco Unified CallManager cluster, and CTI scalability limit is 2500 per provider, the application can open 2500 devices out of 10,000 devices (the number of devices gets configured by using service parameters; see the "CTIManager" section on page 45-2). For CTI super provider applications, these 2500 devices do not remain fixed because applications can close these devices and open another set of 2500 devices, which makes this a variable set of devices (within CTI scalability limits).

The system administrator configures the CTI super provider capability by adding the application user or end user to the Standard CTI Allow Control of All Devices user group. The administrator uses the User Groups Configuration window in Cisco Unified CallManager Administration to add users to user groups.

For information about CTI-controllable devices, see the "CTI-Controlled Devices" section on page 45-3.

All CTI applications with super provider capability exercise control over any CTI-controllable devices in the system. If an application needs to know only the status of a device, it opens the device and gets the status. Because CTI super provider controls any device, you cannot exclude any device from CTI super provider control. CTI system limits determine the maximum number of devices that a CTI application can control. See the "CTIManager" section on page 45-2 for a description of CTI maximum limits. If the limits are exceeded, CTI generates alarms.

If a CTI application monitors a call park number, you must add the application to the Standard CTI Allow Call Park Monitoring user group (see Finding a User Group in the *Cisco Unified CallManager Administration Guide*).

Dependency Records

To find the directory numbers that a specific CTI route point is using, click the Dependency Records link that is provided on the Cisco Unified CallManager Administration CTI Route Point Configuration window. The Dependency Records Summary window displays information about directory numbers that are using the route point. To find out more information about the directory number, click the directory number, 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 and Deleting a CTI Route Point in the *Cisco Unified CallManager Administration Guide*.

CTI Redundancy

CTI provides recovery of failure conditions that result from a failed Cisco Unified CallManager node within a cluster and failure of a CTIManager. This section describes the failover and fallback capabilities of the following components:

- Cisco Unified CallManager
- CTIManager
- Applications (TAPI/JTAPI)

Cisco Unified CallManager

When a Cisco Unified CallManager node in a cluster fails, the CTIManager recovers the affected CTI ports and route points by reopening these devices on another Cisco Unified CallManager node. If an application has a phone device open, the CTIManager also reopens the phone when the phone fails over to a different Cisco Unified CallManager. If the Cisco Unified IP Phone does not fail over to a different

Cisco Unified CallManager, the CTIManager cannot open the phone or a line on the phone. The CTIManager uses the Cisco Unified CallManager group that is assigned to the device pool to determine which Cisco Unified CallManager to use to recover the CTI devices and phones that the applications opened.

When the CTIManager initially detects the Cisco Unified CallManager failure, it notifies the application (JTAPI/TAPI) that the devices on that Cisco Unified CallManager went out of service. If no other Cisco Unified CallManager in the group is available, the devices remain out of service. When those devices successfully rehome to another Cisco Unified CallManager, the CTIManager notifies the application that the devices are back in service.

When a failed Cisco Unified CallManager node comes back in service, the CTIManager rehomes the affected CTI ports/route points to their original Cisco Unified CallManager. The rehoming process starts when calls are no longer being processed or active on the affected device. Because devices cannot be rehomed while calls are being processed or active, the rehoming process may not occur for a long time, especially for route points that can handle many simultaneous calls.

If none of the Cisco Unified CallManagers in the Cisco Unified CallManager group is available, the CTIManager waits until a Cisco Unified CallManager comes into service and tries to open the CTI device again. If for some reason the Cisco Unified CallManager cannot open the device or associated lines when it comes back into service, the CTIManager closes the device and lines.

CTIManager

When a CTIManager fails, the applications that are connected to the CTIManager can recover the affected resources by reopening these devices on another CTIManager. An application determines which CTIManager to use on the basis of CTIManagers that you defined as primary and backup when you set up the application (if supported by the application). When the application connects to the new CTIManager, it can reopen the devices and lines that previously opened. An application can reopen a Cisco Unified IP Phone before the phone rehomes to the new Cisco Unified CallManager; however, it cannot control the phone until the rehoming completes.

Note The applications do not rehome to the primary CTIManager when it comes back in service. Applications fail back to the primary CTIManager if you restart the application or if the backup CTIManager fails.

Application Failure

In the Application Heartbeat Maximum Interval and Application Heartbeat Minimum Interval parameters, you define the interval at which applications send messages to the CTIManager. The CTIManager determines that an application has failed if it does not receive a message from the application in two consecutive intervals. When an application (TAPI/JTAPI or an application that directly connects to the CTIManager) fails, the CTIManager closes the application and redirects unterminated calls at CTI ports and route points to the application that configured the call forward on failure (CFOF) number. The CTIManager also routes new calls into CTI ports and route points that an application does not open to the application CFNA number.

CTI Configuration Checklist

Table 45-1 provides steps to configure Cisco Unified CallManager for CTI applications.

Note To make the CTI application secure, consult the information on configuring authentication and encryption for CTI in the *Cisco Unified CallManager Security Guide*.

Table 45-1 CTI Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Configure the appropriate CTIManager and Cisco CallManager service parameters.	Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
Step 2	Add and configure an IP phone, CTI route points, or ports for each CTI application.	Configuring a CTI Route Point, *Cisco Unified CallManager Administration Guide* Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 3	Configure the directory number for the CTI device.	Configuring a Directory Number, *Cisco Unified CallManager Administration Guide*
Step 4	Associate all devices that the application will use with the appropriate Cisco Unified CallManager group (via the device pool).	Configuring a Device Pool, *Cisco Unified CallManager Administration Guide*
Step 5	Configure the end users and application users that will use CTI applications. Add the device that is used for CTI applications (for example, IP phone, CTI port) to the Controlled Devices list that is on the End User and Application Users Configuration window.	Adding an End User, *Cisco Unified CallManager Administration Guide* Adding an Application User, *Cisco Unified CallManager Administration Guide*
Step 6	Add the end users and application users to the Standard CTI Enabled user group. **Note** All CTI users must be in the Standard CTI Enabled user group, but they may also be in other CTI user groups.	Adding Users to a User Group, *Cisco Unified CallManager Administration Guide*
Step 7	Activate the CTIManager service on the appropriate servers, if not already activated.	*Cisco Unified CallManager Serviceability Administration Guide*
Step 8	Install and configure your applications.	Refer to the documentation that is provided with your application.
Step 9	Restart application engine (if required).	Refer to the documentation that is provided with your application.

Where to Find More Information

Related Topic

- Redundancy, page 7-1

Additional Cisco Documentation

- *Cisco Unified CallManager JTAPI Developer Guide*
- *Cisco TAPI Developer Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Security Guide*

CHAPTER 46

Cisco ATA 186

The Cisco ATA 186 Analog Telephone Adaptor functions as an analog telephone adapter that interfaces regular analog telephones to IP-based telephony networks. The Cisco ATA converts any regular analog telephone into an Internet telephone. Customers install the Cisco ATA at their premises. Each adapter supports two voice ports, each with its own telephone number.

This section covers the following topics:

- Cisco ATA 186 Features, page 46-1
- Connecting with Cisco Unified CallManager, page 46-1
- Configuration Checklist, page 46-2
- Where to Find More Information, page 46-2

Cisco ATA 186 Features

The following list describes the Cisco ATA:

- Contains a single 10 BaseT RJ-45 port and two RJ-11 FXS standard analog telephone ports
- Supports G.711 alaw, G.711 mulaw, and G.723 and G.729a voice codecs
- Uses the Skinny Client Control Protocol
- Converts voice into IP data packets that are sent over a network
- Supports redial, speed dial, call forwarding, call waiting, call hold, transfer, conference, voice messaging, message-waiting indication, off-hook ringing, caller-ID, callee-ID, and call waiting caller-ID

Connecting with Cisco Unified CallManager

Like other IP devices, the Cisco ATA receives its configuration file and list of Cisco Unified CallManagers from the TFTP server. If the TFTP server does not have a configuration file, the Cisco ATA uses the TFTP server name or IP address and port number as the primary Cisco Unified CallManager name or IP address and port number.

After the Cisco ATA initializes, both ports on the Cisco ATA (skinny clients) attempt to connect with the primary Cisco Unified CallManager. If the connection or registration fails, the Cisco ATA skinny clients attempt to register with the next Cisco Unified CallManager in the Cisco Unified CallManager list. If that connection fails, the Cisco ATA skinny clients attempt to register with the last Cisco Unified CallManager in the list. If all attempts to connect and register with a Cisco Unified CallManager fail, the client attempts to connect at a later time.

Upon successful registration, the Cisco ATA client requests the Cisco Unified CallManager software version, current time and date, line status, and call forward status from the Cisco Unified CallManager. If the Cisco ATA loses connection to the active Cisco Unified CallManager, it attempts to connect to a backup Cisco Unified CallManager in the Cisco Unified CallManager list. When the primary Cisco Unified CallManager comes back online, the Cisco ATA attempts to reconnect to it.

Configuration Checklist

Table 46-1 provides steps to configure the Cisco ATA.

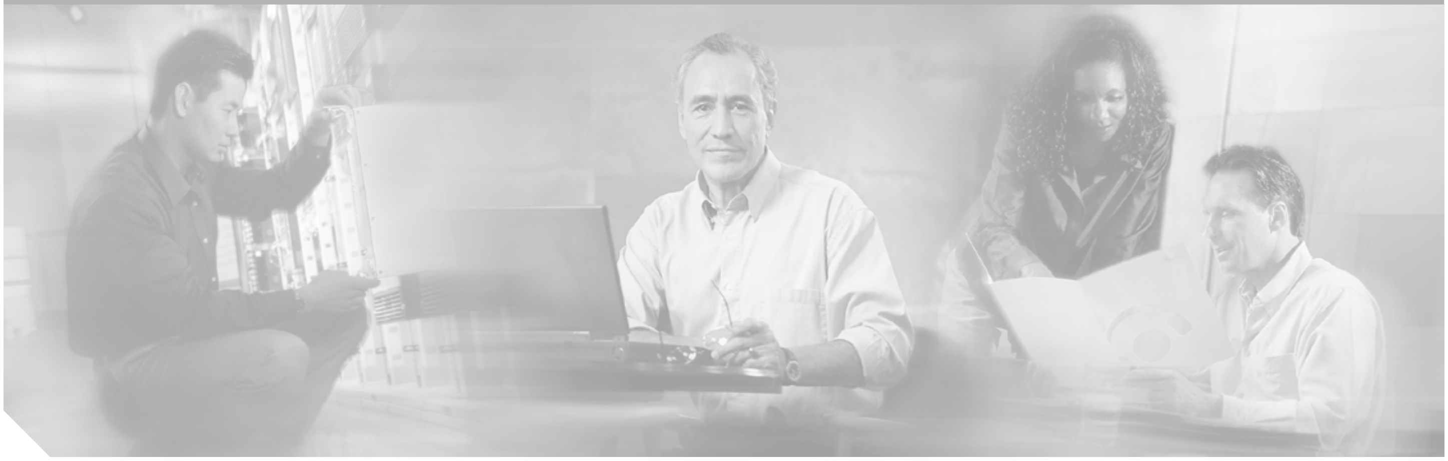
Table 46-1 Cisco ATA 186 Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Configure the Cisco ATA in Cisco Unified CallManager Administration.	Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*
Step 2	Install the Cisco ATA.	Refer to the administration guide that is provided with the product.
Step 3	Make a call.	Refer to the documentation that is provided with the product.

Where to Find More Information

Related Topics

- System-Level Configuration Settings, page 5-1
- Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide*



PART 9

System Maintenance

CHAPTER 47

Administrative Tools Overview

This section provides an overview of the following tools for Cisco Unified CallManager administrators:

- Bulk Administration Tool (BAT), page 47-1
- CDR Analysis and Reporting (CAR), page 47-2
- Cisco Unified CallManager Serviceability, page 47-1
- Call Detail Records, page 47-2
- Where to Find More Information, page 47-3

Bulk Administration Tool (BAT)

The Bulk Administration Tool (BAT), installed with Cisco Unified CallManager, lets you add, update, or delete a large number of phones, users, user device profiles, Cisco Unified CM Assistant managers and assistants, Cisco VG200 gateways and ports, and Cisco Catalyst 6000 24 Port FXS analog interface modules to the Cisco Unified CallManager database. Where this was previously a manual operation, BAT helps you automate the process and achieve much faster add, update, and delete operations.

BAT installs as part of the Cisco Unified CallManager Administration.

For more information, refer to the *Cisco Unified CallManager Bulk Administration Guide.*

Cisco Unified CallManager Serviceability

Administrators can use the Cisco Unified CallManager Serviceability web-based tool to troubleshoot problems with the Cisco Unified CallManager system. Cisco Unified CallManager Serviceability provides the following services:

- Saves Cisco Unified CallManager services alarms and events for troubleshooting and provides alarm message definitions.
- Saves Cisco Unified CallManager services trace information to various log files for troubleshooting. Administrators can configure, collect, and view trace information.
- Monitors real-time behavior of the components in a Cisco Unified CallManager cluster.
- Generates reports for Quality of Service, traffic, and billing information through Cisco CDR Analysis and Reporting (CAR) application.
- Provides feature services that you can activate, deactivate, and view through the Service Activation window.

- Provides an interface for starting and stopping feature and network services.
- Archives reports that are associated with Cisco Unified CallManager Serviceability tools.
- Allows Cisco Unified CallManager to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a server (or all servers in the cluster).

To access Serviceability from the Cisco Unified CallManager Administration window, choose **Serviceability** from the **Navigation** drop-down list box that displays in the upper, right corner of the window.

For more information, refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System Guide*.

CDR Analysis and Reporting (CAR)

CAR, a web-based reporting application, generates reports based on the call detail records (CDRs) and call management records (CMRs) that Cisco Unified CallManager collects. CAR processes the CDR and CMR flat files that the CDR Repository service places in the CDR repository and stores the information in the CAR database. CAR uses the information to generate reports that provide information regarding voice quality, traffic, and billing.

To access CAR, administrators must activate the CAR services in Cisco Unified CallManager Serviceability. After you activate the appropriate services, administrators can access CAR through a secured login from the Cisco Unified CallManager Serviceability Tools menu. End users and managers can access a subset of the reports through a URL that you provide to them.

To view the reports, you must use Adobe Acrobat Reader, which you can download and install from the CAR main window. You can also save reports as CSV files.

For more information, refer to the *CDR Analysis and Reporting Administration Guide*.

Call Detail Records

When CDR collection is enabled through the CDR Enabled Flag Cisco CallManager service parameter, Cisco Unified CallManager writes call detail records (CDRs) to flat files on the subsequent servers as calls are completed. When CDR Diagnostic collection is enabled through the Call Diagnostics Enabled Cisco CallManager service parameter, Cisco Unified CallManager writes call detail diagnostic records to flat files on the subsequent servers as calls are completed. The CDR Repository Manager service maintains the CDR and CMR files, sends files to preconfigured destinations, and manages the disk usage of the files. CAR accesses the CDR/CMR files in the directory structure that the CDR Repository Manager service creates.

Enable and configure CDR collection through service and enterprise parameters that are set in Cisco Unified CallManager Administration. You must enable CDR collection on each Cisco Unified CallManager in the cluster for which you want to generate records.

The following service parameters apply to CDRs:

- CDR Enabled Flag—Cisco CallManager service parameter that controls whether CDRs are generated. Set this parameter on each Cisco Unified CallManager in the cluster. You do not need to restart the Cisco Unified CallManager for the change to take effect.

- CDR Log Calls With Zero Duration Flag—Cisco CallManager service parameter that controls whether calls with zero duration are logged in CDRs. The default specifies False (zero duration calls not logged).
- Call Diagnostics Enabled—Cisco CallManager service parameter that controls whether call diagnostic records that contain QoS information about calls are generated. The default specifies False (diagnostics not generated).

The following enterprise parameters apply to CDRs:

- CDR File Time Interval—The parameter that determines how many seconds to write to a CDR file before Cisco Unified CallManager closes the CDR file and opens a new one.
- Cluster ID—Parameter that provides a unique identifier for the cluster. This parameter gets used in CDR records, so collections of CDR records from multiple clusters can be traced to the sources. The default specifies StandAloneCluster.

Use the CDR Management Configuration window in Cisco Unified CallManager Serviceability to set the amount of disk space to allocate to CDR and CMR files, configure the number of days to preserve files before deletion, and configure up to three billing application server destinations for CDRs.

For more information, see the *Cisco Unified CallManager Serviceability Administration Guide*.

Where to Find More Information

Related Topics

- Cisco TFTP, page 10-1
- Cisco Unified CallManager Attendant Console, page 37-1
- Understanding Cisco Unified CallManager Voice Gateways, page 39-1
- Cisco Unified IP Phones, page 43-1
- Call Admission Control, page 8-1
- System Configuration Checklist, page 5-17
- Device Defaults Configuration, *Cisco Unified CallManager Administration Guide*
- Device Pool Configuration, *Cisco Unified CallManager Administration Guide*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*
- Cisco Unified CallManager Group Configuration, *Cisco Unified CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*

INDEX

A

AAR
  explained 17-1
abbreviated dial
  described 43-25
access log 4-3
access privileges
  roles 4-2
ad hoc conference
  drop conference settings 24-7
  initiating 24-6
  Join softkey 24-7
  limitations 24-9
  SIP phone restrictions 24-8
  using cBarge softkey 24-7
  using conference softkey 24-6
administrator
  tools
    BAT 47-1
    CAR 47-2
    Cisco Unified CallManager Serviceability 47-1
    more information 47-3
    overview 47-1
admission control 5-13, 8-1
alternate routing
  video 44-8
analog telephony protocols
  CAS 40-5
  described 40-3
  E&M signaling 40-4
  ground-start signaling 40-4
  loop-start signaling 40-4
announcements 23-4
announcements (table) 23-4
annunciator 23-1
  announcements 23-4
  announcements (table) 23-4
  configuration checklist (table) 23-5
  dependency records 23-5
  more information 23-6
  overview 23-1
  planning configuration 23-2
  system requirements and limitations 23-3
  tones 23-4
  troubleshooting 23-5
  understanding 23-1
appliance 1-1
application dial rules
  configuration design 19-1
  configuration error checking 19-2
application user
  associating devices 21-3
  configuration checklist (table) 21-5
  described 21-1, 21-2
  more information 21-6
audio quality 8-1
automated alternate routing (AAR)
  dial prefix matrix example (table) 17-3
  enable service parameter 17-3
  example 17-2
  explained 17-1
  line/DN and AAR groups (table) 17-2
autoregistration
  configuration checklist (table) 12-3
  described 12-1

more information 12-4
multiple protocol support 12-2
understanding 12-1

B

balanced call processing
explained 6-3
bandwidth
allocation of 8-1
calculations for admission control 8-4
used by Cisco Unified CallManager 5-7
used by codec types (table) 5-8
barge
described 43-20
Basic Rate Interface (BRI) 40-6
BAT 47-1
Bulk Administration Tool (BAT) 47-1
buttons
directories button 43-28
messages button 43-27

C

call admission control 5-13
gatekeepers
components 8-8
explained 8-6
in a distributed setting (figure) 8-7
locations
explained 8-2
illustrated (figure) 8-2
more information 8-10, 9-23
overview 8-1
trunks 8-6
call completion, QSIG supplementary service
See Cisco Call Back
call control 22-2
call coverage
call forwarding 17-10
described 17-10
hunting 17-10
maximum hunt timer 17-11
personal preferences 17-11
call detail records (CDRs)
described 47-2
video 44-11
call diagnostics and voice quality metrics
described 43-24
call display restrictions
configuring in translation pattern 17-28
call diversion (forwarding), QSIG supplementary service 40-9
called party
transformations 17-25
transformations settings 17-27
transformations settings (table) 17-27
caller identification
restrictions 17-28
support for device control protocols (table) 17-33
support vs. device control protocols 17-32
types 17-28
call failure, avoiding 27-4
call forward
described 17-10, 18-6, 43-20
in multiple voice-mail systems 29-5
multiple voice-mail systems examples 29-6
calling party
presentation settings 17-28
restriction settings 17-28
transformations 17-25
transformations settings 17-25
transformations settings (table) 17-26, 17-29
calling search spaces
dependency records 15-3
examples 15-2
explained 15-1

guidelines and tips 15-3
list of topics 15-1
more information 15-4
search for phones 43-26
call park
described 43-21
call pickup
described 43-21
call pickup group
see features and services 34-1
call preservation
explained 11-4
scenarios (table) 11-5
call processing
balanced load
explained 6-3
by Cisco Unified CallManager 2-2
combined with redundancy (figure) 7-3
calls
making and receiving multiple per directory number 18-7
on-hook call transfer 43-23
video 44-2
call select
described 43-22
call transfer, QSIG supplementary service 40-10
call transfer using hookflash 29-6
call waiting
described 18-7
CAR
overview 47-2
Catalyst 4000
4224 voice gateway switch 39-7
access gateway module 39-7
voice gateway modules 39-5
Catalyst 4224 Voice Gateway Switch 39-7
Catalyst 6000
Cisco Communication Media Module 39-7
configuration illustrated (figure) 28-7
described 28-10
FXS analog interface module 39-6
hookflash transfer 39-6
T1/E1 line card 39-6
voice gateway modules 39-5
Catalyst DSP
more information 28-10
overview 28-1
understanding 28-1
Catalyst MTP 28-2
Catalyst switches
6000 family 28-10
CDR
described 47-2
CDR Analysis and Reporting (CAR) 47-2
centralized TFTP
master centralized TFTP 10-8
overview 10-7
channel associated signaling (CAS) 39-1, 40-5
characters, special
configuring 17-15
described (table) 17-16
Cisco Access Digital Trunk Gateways DT-24+/DE-30+ 39-2
Cisco ATA 186
configuration checklist (table) 46-2
connecting to Cisco Unified CallManager 46-1
more information 46-2
Cisco Call Back
described 40-8
Cisco Communication Media Module (CMM) 39-7
Cisco DPA
illustrated (figure) 32-2
integration overview 32-1
more information 32-3
Cisco IAD2420 Integrated Access Device 39-4
Cisco IP Communicator
default phone button template 43-13
described 43-8

Cisco IP SoftPhone 21-5
Cisco Messaging Interface (CMI) 30-2
Cisco SIP endpoints
  SIP profile 41-19
Cisco SIP IP Phones
  default phone button template (advanced) 43-13
  default phone button template (basic) 43-13
  models supported 43-7
Cisco TFTP service
  alternate paths 10-8
  configuration checklist (table) 10-10
  list of topics 10-1
  more information 10-10
  overview 10-1
  understanding 10-4
Cisco Unified CallManager
  additional documentation 1-3
  bandwidth usage 5-7
  becoming inactive 25-3, 27-5
  benefits 1-2
  call processing 2-2
  configuration, configuring 5-2
  configuring 5-2
  CTI redundancy 45-6
  groups
    configuring 5-3
    described 7-1
    illustrated (figure) 7-2
  introduction 1-1
  key features 1-2
  more information 1-3
  redundancy 7-1
  server, configuring 5-1
  supported voice codecs 5-7
  voice mail connectivity 29-1
Cisco Unified CallManager Assistant
  softkey templates
    described 43-15
Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) 24-3
Cisco Unified CallManager JTAPI
  using user directory 21-1
Cisco Unified CallManager System Guide
  conventions xxv
  organization xxiv
  related documentation xxv
Cisco Unified CallManager User Options 43-28
Cisco Unified Communications
  applications 2-2
  call processing 2-2
  clients 2-3
  components 2-1
  configuring system 3-1
  infrastructure 2-3
  more information 2-4
  network 2-3
  overview 2-1
  support 2-1
Cisco Unified IP Phones
  See also phones
  12 SP+, described 43-7
  30 VIP, described 43-7
  7902, described 43-6
  7905, described 43-5
  7910, described 43-5
  7911, described 43-5
  7912, described 43-4
  7914 Expansion Module, described 43-4
  7920, described 43-4
  7935, described 43-7
  7940, described 43-3
  7941, described 43-3
  7960, described 43-3
  7961, described 43-3
  7970, described 43-2
  7971, described 43-2
  7985, described 43-6

Cisco Unified IP Conference Station 7936, described 43-6
directories button 43-28
features
abbreviated dial 43-25
barge 43-20
call diagnostics and voice quality metrics 43-24
call forward 43-20
call park 43-21
call pickup 43-21
call select 43-22
conference list 43-22
described 43-20
direct transfer 43-22
immediate divert 43-23
join 43-23
malicious call ID 43-23
privacy 43-20
quality report tool 43-23
service URL 43-25
speed dial 43-25
messages button 43-27
overview 43-1
supported models
described (table) 43-2
listed 43-2
Cisco Unified IP Phone Services
configuration checklist (table) 35-3
dependency records 35-3
guidelines and tips 35-2
more information 35-4
overview 35-1
understanding 35-1
Cisco Unity
configuration checklist (table) 31-5
connections with the phone system (figure) 31-2
integrated mailbox configuration 31-4
messaging integration 31-1, 31-2
more information 31-7
system requirements 31-1
Cisco VG200 Voice Gateway 39-2
Cisco VG224 Analog Phone Gateway
configuring 39-4
description 39-4
Cisco VG248 Analog Phone Gateway
configuring 39-2
description 39-2
gateway redundancy 39-14
closest-match routing 17-12
clusters
balanced call processing
explained 6-3
communication between 6-2
compared to groups 7-1
described 6-1
list of topics 6-1
more information 6-4
overview 6-1
CMI
redundancy
described 30-2
illustrated (figure) 30-3
CMLocal date/time group 5-4
codecs
bandwidth used per call (table) 5-8
G.711 5-7
G.723 5-7
G.729 5-7
GSM 5-7
supported by Cisco Unified CallManager 5-7
video 44-2
wideband 5-7
common phone profiles
described 43-19
communication
between clusters 6-2
communication protocols, gateway 39-9
compression of voice stream 28-3

Computer Telephony Integration (CTI) 45-1
conference
ad hoc
initiating 24-6
limitations 24-9
described 18-7
meet me
limitations 24-9
meet-me
initiating 24-9
conference bridge
ad hoc
described 24-6
annunciator 24-4
Cisco IOS configuration settings (table) 24-4
configuration checklist (table) 24-11
dependency records 22-6, 24-9
meet-me
described 24-6
more information 24-11
overview 24-1
performance monitoring 24-10
troubleshooting 24-10
types in Cisco Unified CallManager Administration 24-4
conference devices
Cisco Unified CallManager Conference Bridge (WS-SVC-CMM), described 24-3
hardware
MTP WS-X6608 DSP service card 24-4
software, described 24-3
understanding 24-1
video, described 24-3
conference list
described 43-22
conference routers
described 24-2
conferencing
across an IP WAN 28-3
using Catalyst DSP 28-1
configuration
files for devices 11-2
settings
checklist (table) 5-17
list of topics 5-1
configuration checklist
MGCP BRI 39-18
connected party
presentation settings 17-30
restriction settings 17-30
transformations settings (table) 17-31
conventions xxv
counters
video bridge 44-11
CTI
application failure 45-7
applications 45-1
configuration checklist (table) 45-8
controlled devices 45-3
CTIManager
described 45-2
redundancy 45-7
dependency records 45-6
IP phones 45-3
list of topics 45-1
media termination points 45-2
more information 45-9
ports
described 43-8, 45-3
redundancy 7-4, 45-6
route points 45-3
super provider 45-5
user groups 45-5
user management 45-5

D

date/time groups
  CMLocal 5-4
  described 5-4
DDI 17-13
  configuring 17-18
  explained (table) 17-18
dependency records
  annunciator 23-5
  calling search spaces 15-3
  Cisco Unified IP Phone Services 35-3
  conference bridge 22-6, 24-9
  CTI 45-6
  directory numbers
    described 18-9
  gateways 39-13
  MTP 27-6
  partitions 15-3
  phones
    described 43-29
  system-level settings 5-16
  time periods 16-3
  time schedules 16-3
  transcoders 25-4
device control protocols
  and caller identification support (table) 17-33
device pools
  described 5-10, 11-3
  search for phones 43-26
  updating 5-11
devices
  accessing TFTP server 10-6
  associating to an application user 21-3
  associating to an end user 21-4
  associating with users 21-3
  conference
    Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) 24-3
    software 24-3
    understanding 24-1
    video 24-3
  configuration files 11-2
  CTI control 45-3
  distributing for redundancy 7-3
  firmware loads 11-2
  identifying TFTP server 10-6
  MTP
    characteristics 27-4
  support
    list of topics 11-1
    more information 11-6
  supported 11-1
  transcoders
    resetting 25-4
  updating firmware loads 11-3
  using Cisco TFTP 10-4
  using DHCP 10-4
DHCP
  alarms 13-4
  and devices 10-4
  DNS 13-2
  migration 13-4
  more information 13-4
  server 13-1
    configuration process 13-3
  TFTP 13-3
dial plans
  accessing gateways 39-12
dial rules
  more information 19-8
  overview 19-1
digital signal processor (DSP) 28-1
digital telephony protocols
  BRI 40-6
  described 40-5
  E1 PRI 40-6
  QSIG 40-6

T1 PRI 40-6

digital trunk gateway

DT-24+/DE-30+ 39-2

digit analysis

static

caveats 17-14

configuration tip 17-13

described 17-13

example prior to static digit analysis 17-15

explained 17-13

Unified CallManager Assistant example with static digit analysis 17-15

directories button

configuring 43-28

directory

access 20-3

access for Cisco IP telephony endpoints 20-5

configuration checklist (table) 20-6

extension mobility 21-4

LDAP 5-12

more information 20-7

overview 20-1

directory lookup dial rules

overview 19-3

directory numbers

active check box 18-5

call forward

busy trigger 18-6, 43-21

no answer ring duration 18-6, 43-21

call forward information display 18-6, 43-21

characteristics 18-1

conference 18-7

configuration checklist (table) 18-9

dependency records

described 18-9

direct transfer 18-7

features 18-5

call forward 18-6

call waiting 18-7

find all directory numbers 18-9

join 18-7

making and receiving multiple calls 18-7

managing 18-5

more information 18-10

overview 18-1

search tips 18-8

shared line appearance 18-2

shared line appearance restrictions 18-4

transfer 18-7

update directory number of all devices sharing this line check box 18-5

direct transfer

described 18-7, 43-22

discard digits instructions (DDI) 17-13

configuring 17-18

explained (table) 17-18

DNs

characteristics 18-1

overview 18-1

document

conventions xxv

organization xxiv

documentation

related xxv

DPA 7630/7610

functionality 32-2

illustrated (figure) 32-2

purpose 32-2

understanding 32-1

using SMDI 32-2, 32-3

DSCP marking 44-8

E

E&M signaling

delay dial 40-4

immediate start 40-4

wink start 40-4

E1 CAS 40-5

E1 Primary Rate Interface (E1 PRI) 40-6

E1 Primary Rate Interface (PRI) 39-1

Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter 4-3

end user

- associating devices 21-4
- configuration checklist (table) 21-5
- described 21-1, 21-2
- more information 21-6

enterprise parameters

- described 5-15
- Effective Access Privileges For Overlapping User Groups and Roles 4-3
- user groups 4-3

expansion module

- Cisco Unified IP Phone 7914 43-4

extension mobility

- described 36-1
- user device profile 21-4
- user directory 21-4

external route plan wizard

- described 17-33
- generated route filters 17-34
- generated route groups 17-35
- generated route lists 17-35
- generated route patterns 17-36

F

features

- call park 33-1
- Cisco Unified CallManager Assistant 38-1
- Cisco Unified IP Phone Services
- extension mobility
  - overview 36-1
- music on hold (MOH) 26-1
- phone features (table) 43-14
- phone login
  - overview 36-1

fields

- requiring route patterns (table) 17-17

firmware loads

- described 11-2
- updating 11-3

Foreign Exchange Office (FXO) 39-1, 39-10, 40-3

Foreign Exchange Station (FXS) 39-1, 39-10, 40-3

FXO 39-1, 39-10, 40-3

FXS 39-1, 39-10, 40-3

G

G.711 5-7

G.723 5-7

G.729 5-7

gatekeepers

- and call admission control (figure) 8-7
- configuration checklist (table) 8-10
- configuring 8-8
- configuring in Cisco Unified CallManager 8-9, 42-2
- configuring on the router 8-8
- described 8-6

gateways

- Catalyst 4000 Access Gateway Module 39-7
- Catalyst 4224 gateway 39-7
- Catalyst 6000
  - configuration illustrated (figure) 28-7
- Catalyst 6000 FXS Analog Interface Module 39-6
- Catalyst 6000 T1/E1 and Services Module 39-6
- Cisco Communications Media Module 39-7
- Cisco IOS H.323 devices 39-7
- Cisco voice gateways 39-1
- communication protocols (table) 39-9
- configuration checklist (table) 39-16
- dependency records 39-13
- failover and fallback 39-13
- H.323 devices list 39-7

models (table) 39-9
more information 39-18
overview 39-1
port types (table) 39-9
related to dial plans 39-12
standalone
digital trunk 39-2
IAD2420 39-4
VG200 voice 39-2
VG224 analog phone 39-4
VG248 analog phone 39-2
summary of voice gateways (table) 39-9
trunk interfaces
table 39-9
Global Directory
displaying with directories button 43-28
ground-start signaling 40-4
groups, Cisco Unified CallManager
compared to clusters 7-1
components of 7-1
configuring 5-3
illustrated (figure) 7-2
groups, date/time 5-4
GSM 5-7

H

H.323
Cisco IOS gateways 39-7
clients 43-8
gateways 39-7
IOS gateway redundancy 39-14
used in voice gateways 40-1
video 44-4
hookflash transfer 39-6
hub-and-spoke topology 8-1
hunting
described 17-10
example 17-11
maximum hunt timer 17-11
personal preferences 17-11
hunt lists
described 17-9
hunt pilots
described 17-9
wildcards 17-16

I

identification services
QSIG supplementary service, described 40-11
immediate divert
described 43-23
intercluster
communication 6-2
voice mail 29-2
internet
ecosystem 2-1
introduction
to Cisco Unified CallManager 1-1
IP Phones
See Cisco Unified IP Phones
IP Phone Services
See Cisco Unified IP Phone Services
IP SoftPhone, Cisco
user directory 21-5
IP telephony
protocols
more information 40-15
understanding 40-1

J

join
described 18-7, 43-23
JTAPI
See Cisco Unified CallManager JTAPI

L

LDAP
- described 5-12
- directory
  - more information 20-7
- overview 20-1

licensing
- alarms 14-3
- migrating from 5.0(x) to 4.0(x) 14-3
- more information 14-4
- overview 14-1
- splitting licenses 14-2
- starting a license manager service 14-1
- transferring licenses 14-4

line groups
- described 17-8

load, firmware 11-2

load balancing
- distributing devices 7-3
- explained 6-3

locations
- and call admission control (figure) 8-2
- and regions 5-9
- configuration checklist (table) 8-6, 9-12
- described 8-2
- interaction with regions 8-3
- interaction with regions (figure) 8-4
- used in admission control 8-1
- video 44-8

loop-start signaling 40-4

M

malicious call ID
- described 43-23

master centralized TFTP
- configuration tips 10-9
- sending files to the master CTFTP server 10-8

maximum hunt timer 17-11

media control 22-2

Media Gateway Control Protocol (MGCP) 40-2

media resource group lists
- configuration checklist (table) 22-6
- described 22-4

media resource groups
- configuration checklist (table) 22-6
- described 22-3

media resource manager
- managing MTPs 27-2
- using to manage transcoders 25-2

media resources
- call control 22-2
- described 22-1
- management 22-1
- media control 22-2
- media resource group lists 22-4
- media resource groups 22-3
- media termination point control 22-2
- more information 22-7
- music on hold control 22-3
- overview 22-1
- redundancy 7-4
- unicast bridge control 22-3

media termination point (MTP) 27-1
- CTI 45-2

media termination point control 22-2

meet-me conference
- limitations 24-9

messages button 43-27

message waiting
- description 29-4
- indication 29-4

messaging
- Cisco Unity
  - integration description 31-2
  - integration overview 31-1

MGCP
- described 40-2
- gateway redundancy 39-13
- gateways using 39-11

MGCP BRI
- configuring 39-18
- illustration of call flow 39-5

MLPP
- described 5-15

modifying files 10-9

MOH
- described 26-1
- MOH control 22-3

MTP
- avoiding call failure/user alert 27-4
- Cisco Unified CallManager becomes inactive 27-5
- configuration checklist (table) 27-7
- CTI 45-2
- dependency records 27-6
- device characteristics 27-4
- failover and fallback 27-5
- managing with media resource manager 27-2
- more information 27-7
- overview 27-1
- planning configuration 27-3
- resetting registered devices 27-6
- system requirements and limitations 27-5
- transcoding services 28-2
- types (table) 27-3
- understanding 27-1
- using transcoders 25-2
- WS-X6608 DSP service card 24-4

multisite WAN
- using centralized MTP transcoding (figure) 28-4

music on hold (MOH)
- described 26-1

N

network
- video 44-3

O

on-hook call transfer 43-23

organization xxiv

overview
- of Cisco Unified CallManager 1-1
- of dial rules 19-1
- of system configuration 3-1

P

parameters
- enterprise
  - described 5-15
  - Effective Access Privileges For Overlapping User Groups and Roles 4-3
- service
  - described 5-16
  - Maximum Phone FallBack Queue Depth 43-28
  - Message Waiting Lamp Policy 29-5

parameters, enterprise
- user groups 4-3

partitions
- dependency records 15-3
- examples 15-2
- explained 15-1
- guidelines and tips 15-3
- list of topics 15-1
- more information 15-4
- name limitations 15-4

path replacement
- described 40-13

performance monitoring counters
- video 44-10

personal preferences 17-11

phone button templates

- 12 series, default template 43-13
- 30 SP+, default template 43-12
- 30 VIP, default template 43-13
- 7902, default template 43-12
- 7905 SCCP, default template 43-12
- 7905 SIP, default template 43-12
- 7910, default template 43-12
- 7911 SCCP, default template 43-12
- 7911 SIP, default template 43-12
- 7912 SCCP, default template 43-12
- 7912 SIP, default template 43-12
- 7920, default template 43-11
- 7940 SCCP, default template 43-11
- 7940 SIP, default template 43-11
- 7941 G-GE SCCP, default template 43-11
- 7941 SCCP, default template 43-11
- 7941 SIP, default template 43-11
- 7960 SCCP, default template 43-11
- 7960 SIP, default template 43-11
- 7961 G-GE SCCP, default template 43-11
- 7961 SCCP, default template 43-11
- 7961 SIP, default template 43-11
- 7970 SCCP, default template 43-10
- 7970 SIP, default template 43-10
- 7971 SCCP, default template 43-10
- 7971 SIP, default template 43-10
- 7985, default template 43-10
- analog phone, default template 43-13
- ATA 186, default template 43-13
- Cisco IP Communicator, default template 43-13
- CN622, default template 43-13
- conference station 7935, default template 43-12
- conference station 7936, default template 43-12
- IP-STE, default template 43-13
- ISDN BRI Phone, default template 43-13
- third-party SIP device, default template 43-13
- VGC phone, default template 43-13
- VGC Virtual, default template 43-13

phone login

- described 36-1

phone NTP reference

- configuring for SIP phones 5-4

phones

- *See also* Cisco Unified IP Phones
- administration tips 43-25
- associating with users 43-25
- button templates
  - default 43-10
  - described 43-9
  - guidelines 43-13
  - listed by model (table) 43-10
- Cisco Unified IP Phone Services 35-1
- common phone profiles 43-19
- dependency records
  - described 43-29
- failover and fallback 43-29
- features
  - described (table) 43-14
  - privacy 43-20
- find all phones 43-27
- methods for adding 43-19
- more information 43-33
- SCCP configuration checklist (table) 43-29
- search by authentication string 43-27
- search by calling search space 43-26
- search by call pickup group 43-26
- search by description 43-26
- search by device name 43-26
- search by device pool 43-26
- search by device protocol 43-27
- search by device type 43-26
- search by directory number 43-26
- search by LSC status 43-26
- search by security profile 43-27
- search tips 43-26
- search within results 43-27

SIP configuration checklist (table) 43-29
softkey templates
add application 43-16
configure softkey layout 43-17
described 43-15
PLAR
for Cisco SIP phones 41-18
ports
configuring for SMDI 30-2
CTI
described 43-8
presentation settings
calling party 17-28
connected party 17-30
preservation of calls
explained 11-4
scenarios (table) 11-5
privacy
described 43-20
private line automatic ringdown
for Cisco SIP phones 41-18
SIP dial rules 19-7
privileges
roles 4-2
profiles
common phone 43-19
protocols
analog telephony 40-3
H.323 29-2, 40-1
MGCP 40-2
Session Initiation Protocol (SIP) 40-3
Skinny Client Control Protocol 39-3, 40-2
Skinny Client Control Protocol (SCCP) Gateway Protocol 39-14
Skinny Gateway Protocol 39-12

Q

QSIG
Annex M.1 40-7
basic call feature 40-8
basic call setup 40-8
call completion 40-8
call diversion (rerouting) 40-9
CallManager interface 40-15
call transfer 40-10
compatibility with older versions (ECMA) 40-10
facility selection and reservation 40-11
identification services 40-11
message tunneling 40-7
message waiting indication (MWI) service 40-13
overview 40-6
path replacement 40-13
supplementary services
call diversion (forwarding) 40-9
Q signaling (QSIG) 39-1, 40-6
QSIG protocol
supplementary services
call completion (Cisco Call Back), described 40-8
call transfer 40-10
identification 40-11
path replacement 40-13
QSIG trunk interface 39-1
quality of sound 8-1
quality report tool
described 43-23

R

redundancy
and distributed call processing (figure) 7-3
Cisco Unified CallManager 45-6
Cisco VG248 39-14
CMI
described 30-2

illustrated (figure) 30-3
CTI 45-6
CTIManager 45-7
IOS H.323 gateways 39-14
list of topics 7-1
MGCP gateway 39-13
more information 7-4
of CTI 7-4
of media resources 7-4
support for gateways 39-13
types of 7-1
with distributed call processing 7-3
regions
and call admission control 5-9
and locations 5-9
described 5-5
example (figure) 5-9
interaction with locations 8-3
interaction with locations (figure) 8-4
used with admission control 8-3
used with admission control (figure) 8-4
video 44-8
related documentation xxv
requirements
Cisco Unity 31-1
restriction settings
calling party 17-28
connected party 17-30
roles
access privileges 4-2
described 4-1, 4-2
more information 4-4
overview 4-1
standard 4-4
route filters
associated with route lists (table) 17-34
described 17-34
route groups
described 17-5
generated 17-35
related to dial plans 39-12
route lists
associated route filters (table) 17-34
described 17-5
generated 17-35
types (table) 17-36
types, example 17-5
route patterns
closest-match routing 17-12
considerations for using 17-6
explained 17-6
fields in Cisco Unified CallManager (table) 17-17
generated with external route plan wizard 17-36
usage 17-6
using the @ wildcard character 17-12
wildcards 17-16
route plans
and Cisco Analog Access Gateways (figure) 17-8
and Cisco Digital Access Gateways (figure) 17-7
external route plan wizard
generated route filters 17-34
generated route groups 17-35
generated route lists 17-35
generated route patterns 17-36
list of topics 17-1
more information 17-37
overview 17-4
report 17-37
routers
conference
hardware 24-2
routing
automated alternate 17-1
closest-match 17-12
time-of-day 16-1
dependency records 16-3
for end users 16-2
more information 16-3

time periods 16-1
time schedules 16-2
understanding 16-1

S

SCCP auto-registration 12-2
search
by authentication string 43-27
by calling search space 43-26
by call pickup group 43-26
by description 43-26
by device name 43-26
by device pool 43-26
by device protocol 43-27
by device type 43-26
by directory number 18-8, 43-26
by LSC status 43-26
by security profile 43-27
for all directory numbers in the database 18-9
for all phones in the database 43-27
for directory numbers 18-8
for phones 43-26
within results 43-27
security profile
search for phones 43-27
server, Cisco Unified CallManager
configuring 5-1
Serviceability
and video 44-10
service parameters
Automated Alternate Routing Enable 17-3
described 5-16
Maximum Phone FallBack Queue Depth 43-28
Message Waiting Lamp Policy 29-5
service URL
described 43-25
Session Initiation Protocol (SIP)
understanding 41-1
settings
called party transformations
configuring 17-27
explained (table) 17-27
calling party transformations
explained (table) 17-26, 17-29
configuring
checklist (table) 5-17
described 5-1
connected party transformations
explained (table) 17-31
special characters 17-15
shared line appearance
active check box 18-5
described 18-2
restrictions 18-4
update directory number of all devices sharing this line check box 18-5
Simplified Message Desk Interface (SMDI) 29-2, 30-1
SIP
3PCC 41-15
ad hoc conference settings 24-8
basic calls 41-6
call identification services 41-9
Cisco Unified CallManager support for Cisco SIP endpoints 41-15
configuration checklist (table) 41-13
description of Cisco CallManager and SIP 41-2
diversion header 41-16
DTMF Relay calls 41-6
functions and features in Cisco Unified CallManager 41-5
join header 41-16
more information 41-20
networking 41-1
protocol 40-3
REFER 41-16
remotecc 41-17
remote party ID (RPID) header 41-16
replaces and referred-by headers 41-16

replaces header 41-16
RFC3261 41-15
RFC3262 41-15
RFC3264 41-15
RFC3265 + dialog package 41-17
RFC3265 + KPML package 41-17
RFC3265 + presence package 41-17
RFC3265 + RFC3842 MWI package 41-17
RFC3311 41-15
RFC3514 41-16
RNDIS 41-12
service parameters 41-3
supplementary services 41-8
understanding 41-1
using MTP devices 41-3
SIP autoregistration 12-2
SIP dial rules
dial rule parameters 19-5
dial rule patterns 19-4
overview 19-4
PLAR 19-7
SIP endpoints
overview 41-13
SIP phone
NTP reference 5-4
PLAR 41-18
SIP phones
See Cisco SIP IP Phones
SIP profile
Cisco SIP endpoints 41-19
SIP trunks 41-5
SIP standards
Cisco endpoints 41-15
SIP trunks
SIP profile 41-5
Skinny Client Control Protocol 39-3, 40-2
Skinny Client Control Protocol (SCCP) Gateway Protocol 39-14
Skinny Gateway Protocol 39-12
SMDI
configuration checklist (table) 30-4
integration requirements 30-1
migration with DPA 7630/7610 32-2, 32-3
more information 30-5
port configuration 30-2
PSTN gateway interfaces 29-2
voice mail integration 29-2, 30-1
softkey templates
call states described (table) 43-17
layout (figure) 43-18
operation 43-18
softphone 43-8
SoftPhone, Cisco IP 21-5
sound quality 8-1
special characters
configuring 17-15
described (table) 17-16
explained 17-16
speed dial
described 43-25
standard roles 4-4
standards
SIP 41-15
standard user groups 4-4
static digit analysis
caveats 17-14
configuration tip 17-13
described 17-13
example prior to static digit analysis 17-15
explained 17-13
Unified CallManager Assistant example with static digit analysis 17-15
supported devices 11-1
system configuration
for complete IP telephony system
overview 3-1
overview checklist (table) 3-1
more information 3-4

overview 3-1

system-level configuration settings 5-1

T

T1 CAS 40-5

T1 Primary Rate Interface (PRI) 39-1

T1 Primary Rate Interface (T1 PRI) 40-6

templates, phone button

- 12 series, default 43-13
- 30 SP+, default 43-12
- 30 VIP, default 43-13
- 7902, default 43-12
- 7905 SCCP, default 43-12
- 7905 SIP, default 43-12
- 7910, default 43-12
- 7911 SCCP, default 43-12
- 7911 SIP, default 43-12
- 7912 SCCP, default 43-12
- 7912 SIP, default 43-12
- 7920, default 43-11
- 7940 SCCP, default 43-11
- 7940 SIP, default 43-11
- 7941 G-GE SCCP, default 43-11
- 7941 SCCP, default 43-11
- 7941 SIP, default 43-11
- 7960 SCCP, default 43-11
- 7960 SIP, default 43-11
- 7961 G-GE SCCP, default 43-11
- 7961 SCCP, default 43-11
- 7961 SIP, default 43-11
- 7970 SCCP, default 43-10
- 7970 SIP, default 43-10
- 7971 SCCP, default 43-10
- 7971 SIP, default 43-10
- 7985, default 43-10
- analog phone, default 43-13
- ATA 186, default 43-13
- Cisco IP Communicator, default 43-13
- CN622, default 43-13
- conference station 7935, default 43-12
- conference station 7936, default 43-12
- default 43-10
- described 43-9
- guidelines 43-13
- IP-STE, default 43-13
- ISDN BRI phone, default 43-13
- listed by model (table) 43-10
- third-party SIP device, default 43-13
- VGC phone, default 43-13
- VGC Virtual, default 43-13

templates, softkey

- add application 43-16
- configure softkey layout 43-17
- described 43-15
- layout (figure) 43-18
- operation 43-18

TFTP 10-8

- alternate Cisco file server fields 10-8
- alternate paths 10-8
- centralized TFTP 10-7, 10-8, 10-9
- configuration checklist (table) 10-10
- configuration files 11-2
- configuration tips
  - alternate Cisco file server fields 10-9
- configuring a backup or fallback server 10-7
- customizing files 10-9
- list of topics 10-1
- master centralized TFTP 10-8
- more information 10-10
- multiple cluster environment 10-7
- overview 10-1
- process overview for Cisco SIP IP phones 10-3
- process overview for SCCP devices 10-2
- server
  - accessing 10-6
  - identifying 10-6
- understanding 10-4

time-of-day routing 16-1
- dependency records 16-3
- for end users 16-2
- more information 16-3
- time periods 16-1
- time schedules 16-2
- understanding 16-1

time periods
- dependency records 16-3
- explained 16-1
- more information 16-3

time schedules
- dependency records 16-3
- explained 16-2
- more information 16-3

time zones 5-4

tones 23-4

tools
- administrator
  - BAT 47-1
  - CAR 47-2
  - Cisco Unified CallManager Serviceability 47-1
  - more information 47-3
  - overview 47-1

transcoders
- configuration checklist (table) 25-5
- dependency records 25-4
- failover and fallback 25-3
- managing with media resource manager 25-2
- more information 25-5
- overview 25-1
- performance monitoring 25-4
- resetting registered devices 25-4
- troubleshooting 25-4
- types in Cisco Unified CallManager Administration 25-2
- understanding 25-1
- using as MTPs 25-2

transcoding
- centralized MTP and conferencing services (figure) 28-4
- IP-to-IP packet 28-3
- IP-to-IP packet across trunks 28-4
- IP-to-IP packet and voice compression 28-3
- using Catalyst DSP 28-1

transfer
- described 18-7
- on-hook 43-23

transformations
- called party 17-25
- calling party 17-25

translation patterns
- and called party transformations settings 17-27
- and calling party presentation and restriction settings 17-28
- and calling party presentation settings (table) 17-29
- and connected party presentation and restriction settings 17-30
- and connected party presentation settings (table) 17-31
- and route plan report 17-37
- use for failover 17-13

Trivial File Transfer Protocol (TFTP) 10-1

troubleshooting
- annunciator 23-5

trunk interfaces
- BRI 40-6
- E1 CAS 40-5
- E1 PRI 39-1, 40-6
- FXO 39-1, 40-3
- FXS 39-1, 40-3
- QSIG 39-1, 40-6
- signaling
  - E&M 40-4
  - ground start 40-4
  - loop start 40-4
- T1 CAS 39-1, 40-5
- T1 PRI 39-1, 40-6

trunks
- associated route groups 42-6
- configuration 42-1
- configuration checklist (table) 8-10, 42-6
- configuring in Cisco Unified CallManager 8-9, 42-2
- configuring on the router 8-8
- dependency records 42-6
- described 8-6
- gatekeeper controlled 42-2
- H.225 gatekeeper controlled 42-3
- intercluster gatekeeper controlled 42-3
- intercluster non-gatekeeper controlled 42-3
- more information 42-7
- non-gatekeeper controlled 42-2
- overview 42-1
- SIP 42-3

U

unicast bridge control 22-3

Unity, Cisco
- *See* Cisco Unity

user
- application
  - associating devices 21-3
  - configuration checklist (table) 21-5
  - described 21-1, 21-2
  - more information 21-6
- configure phone features 43-28
- end
  - associating devices 21-4
  - configuration checklist (table) 21-5
  - described 21-1, 21-2
  - more information 21-6

user alert, avoiding 27-4

user directory
- extension mobility 21-4

user groups
- CTI 45-5
- described 4-1, 4-3
- enterprise parameters 4-3
- more information 4-4
- overview 4-1
- standard 4-4

user management
- CTI 45-5

user options
- Cisco Unified CallManager User Options 43-28

V

video
- alternate routing 44-8
- and Serviceability 44-10
- bandwidth management 44-7
- bridge counters 44-11
- call details records 44-11
- calls 44-2
- codecs 44-2
- conference devices 24-3
- configuration checklist (table) 44-12
- DSCP marking 44-8
- H.323 44-4
- locations 44-8
- more information 44-13
- network 44-3
- other configuration 44-9
- performance monitoring counters 44-10
- phone configuration 44-9
- regions 44-8
- Skinny Client Control Protocol 44-6
- Skinny Client Control Protocol bridging 44-6
- understanding 44-1

video phones
- Cisco Unified IP Phone 7985 43-6

voice codecs
- bandwidth used per call (table) 5-8
- G.711 5-7

G.723 5-7

G.729 5-7

GSM 5-7

supported by Cisco Unified CallManager 5-7

wideband 5-7

voice compression 28-3

voice gateways, see gateways

voice mail

access 29-2

gateway-based 29-2

call forwarding

intercluster trunk, example 29-6

intracluster trunk, examples 29-6

call forwarding in multiple systems 29-5

call transfer 29-6

configuration

message waiting indication 29-4

message-waiting indication policy 29-4

more information 29-7

configuring messages button 43-27

connectivity

more information 29-7

connectivity to Cisco Unified CallManager 29-1

gateway-based 29-2

interfaces 29-1

intercluster 29-2

PSTN gateway 29-2

Skinny Protocol 29-2

message waiting configuration 29-4

pilot numbers 29-3

profiles 29-3

SMDI

configuration checklist (table) 30-4

integration 30-1

requirements for integration 30-1

voice messaging, see voice mail

voice quality 8-1

W

wideband 5-7

wildcards

described (table) 17-16

for hunt pilots 17-16

for route patterns 17-16

using @ in route patterns 17-12