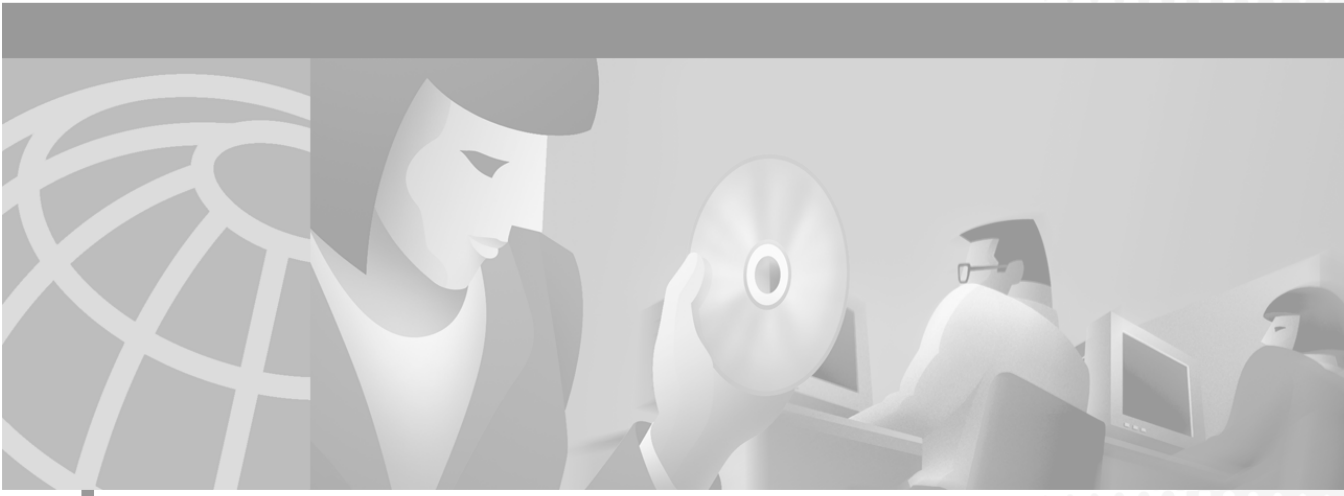


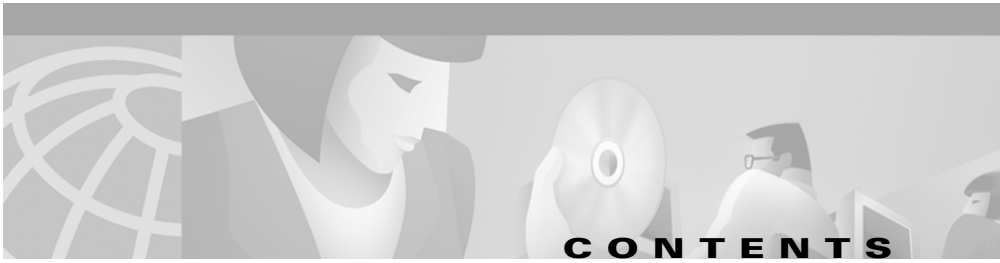
Cisco CallManager System Guide

Release 3.1

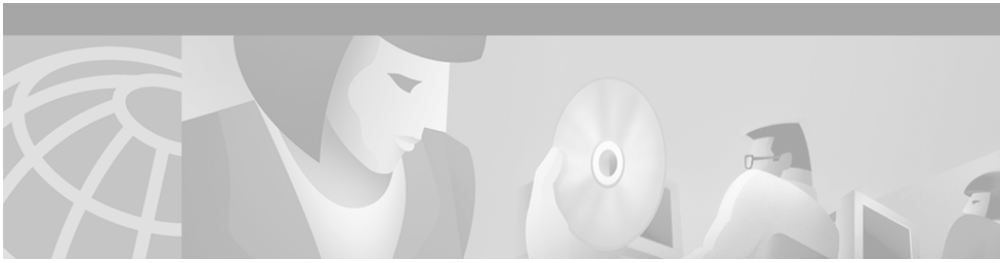
Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7813341=
Text Part Number: 78-13341-01

Cisco CallManager System Guide



CONTENTS



Preface

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

The preface covers these topics:

Purpose

The *Cisco CallManager System Guide* provides information about administering the Cisco CallManager system.

Audience

The *Cisco CallManager System Guide* is written for network administrators responsible for managing the Cisco 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 CallManager" Provides an overview of Cisco CallManager and Cisco IP telephony network components.
Part 2	"Understanding Cisco CallManager System Configuration" Details the basic configuration flow for a Cisco CallManager system and explains system-level configuration concepts and settings.
Part 3	"Dial Plan Architecture" Describes route plans, partitions, and calling search spaces.
Part 4	"LDAP Directory and User Configuration" Provides information about the LDAP directory and user directory configuration.
Part 5	"Media Resources" Explains how to manage and configure media resources for transcoding, conferencing, media termination points, and music on hold.
Part 6	"Voice Mail and Messaging Integration" Discusses how to integrate voice mail and messaging applications with Cisco CallManager.
Part 7	"System Features" Describes additional system-wide features such as call park, extension mobility, and custom phone rings.

Part	Description
Part 8	"Voice Gateways, Phones, and Computer Telephony Integration" Explains how to integrate gateways, phones, and software applications with your Cisco CallManager system.
Part 9	"System Maintenance" Describes tools as well administrative passwords and accounts for your Cisco CallManager system.

Related Documentation

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

- *Installing Cisco CallManager Release 3.1*
- *Release Notes for Cisco CallManager Release 3.1*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco IP Phone 7900 Family Administration Guide*
- *Balk Administration Tool Guide for Cisco CallManager*

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.

Convention	Description
[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:

Tips 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

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

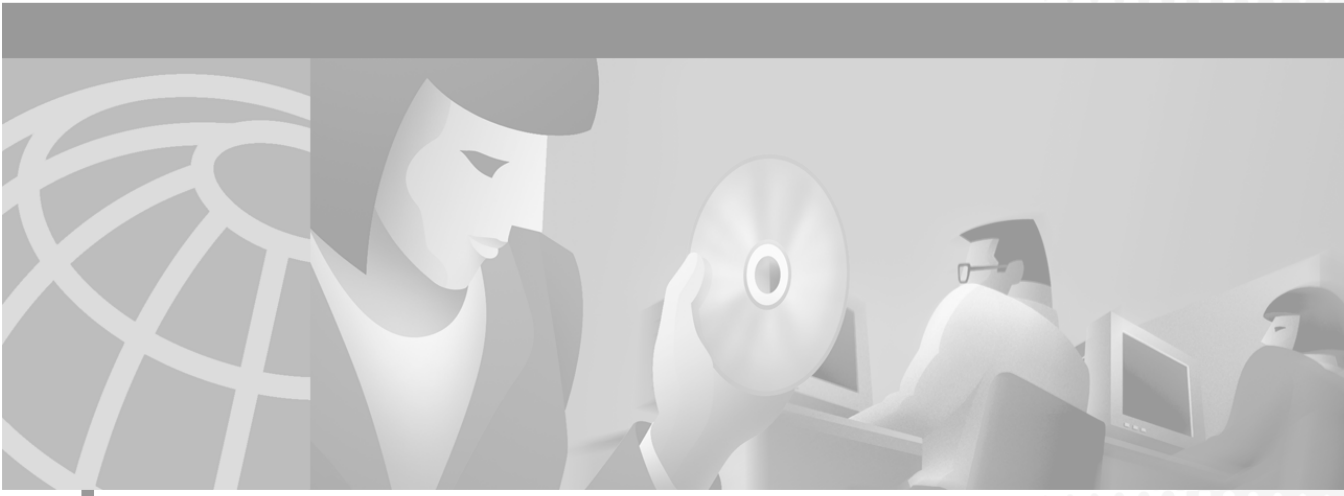
Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



PART 1

Understanding Cisco CallManager

CHAPTER 1

Introduction

Cisco CallManager serves as the software-based call-processing component of the Cisco IP Telephony Solution for the Enterprise part of Cisco AVVID (Architecture for Voice, Video and Integrated Data). The Cisco Media Convergence Server (MCS) provides a high-availability server platform for Cisco CallManager call processing, services, and applications.

The Cisco 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 CallManager open telephony application program interface (API).

Cisco CallManager provides signaling and call control services to Cisco integrated telephony applications as well as 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 SoftPhone, Cisco IP Interactive Voice Response (IP IVR), Cisco Personal Assistant, and Cisco WebAttendant

Key Features and Benefits

The Cisco CallManager system includes a suite of integrated voice applications that perform voice conferencing and manual attendant console functions. This suite of voice applications means no need exists for special-purpose voice-processing hardware. 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 CallManager is a software application, enhancing its capabilities in production environments only requires upgrading software on the server platform, thereby avoiding expensive hardware upgrade costs.

Distribution of Cisco CallManager and all Cisco 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 link and automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available. Cisco Media Convergence Server comes with Cisco CallManager preinstalled.

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 CallManager Administration Guide*
- *Cisco IP Telephony Network Design Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network/

CHAPTER 2

Cisco IP Telephony Overview

Multiple communication networks today are entirely separate, 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 has 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 connecting their disparate PBXs via their wide-area data network to avoid long-distance charges.

By converging these previously disparate networks into a single, unified network, you can begin to realize savings in multiple areas, including lower total cost of ownership, toll savings, and increased productivity.

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

Cisco Architecture for Voice, Video, and Integrated Data (Cisco AVVID)

Cisco AVVID encompasses the following components:

- Converged client devices
- Hardware/software
- Directory services
- Call processing
- Telephony/data applications
- Network management
- Service and support

Cisco AVVID 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 AVVID 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 gives some voice and video applications in the application layer of Cisco AVVID:

- Cisco Unity—The Cisco Unity messaging application provides voice-messaging to enterprise communications.
- Video—IP-TV and IP-video conferencing products enable distance learning and workgroup collaboration.
- Cisco IP IVR—As an IP-powered interactive voice response (IVR) solution, Cisco IP IVR combined with Cisco IP AutoAttendant, provides an open and feature-rich foundation for delivering IVR solutions over an IP network.
- Cisco WebAttendant—This flexible and scalable application replaces the traditional PBX manual attendant console.
- Cisco IP SoftPhone—The Cisco IP SoftPhone, a software, computer-based phone, provides communication capabilities that increase efficiency and promote collaboration.
- Personal Assistant—Personal Assistant selectively handles calls and helps you make outgoing calls. Personal Assistant provides rule-based call routing, speech-enabled directory dialing, voice mail browsing, and simple ad-hoc conferencing.

Call Processing

Cisco CallManager, a software-only call-processing application, distributes calls and features; and clusters phones, regions, groups, etc., over an IP network; allowing scalability to 10,000 users and triple call processing redundancy.

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

Infrastructure

The following list shows the components of the infrastructure layer of Cisco AVVID:

- Media convergence servers
- General voice products for Cisco IP Telephony Solutions
- Switches
- Integrated IP telephony solution
- Voice trunks
- Voice gateways
- Toll bypass products

Clients

Cisco delivers the following IP-enabled communication devices:

- Cisco IP Phone 7960
- Cisco IP Phone 7940
- Cisco IP Phone 7910
- Cisco IP Conference Station 7935
- Cisco IP SoftPhone
- Cisco Sidecar 79xx

Cisco IP Telephony Network

The Cisco IP Telephony network includes the following components:

- Cisco CallManager
- Cisco IP phones
- IOS platforms
- Digital gateways

- Analog gateways
- Transcoders
- Conferencing (hardware/software)
- Media Termination Point
- Music On Hold
- Inline power modules (10/100 Ethernet switching modules)
- Cisco IP SoftPhone

Control from the Cisco IP phone to Cisco CallManager uses Skinny Station Protocol and, independently, desktop computer to Cisco CallManager, as an H.323 gatekeeper using H.225/H.245 over TCP.

Where to Find More Information

Related Topics

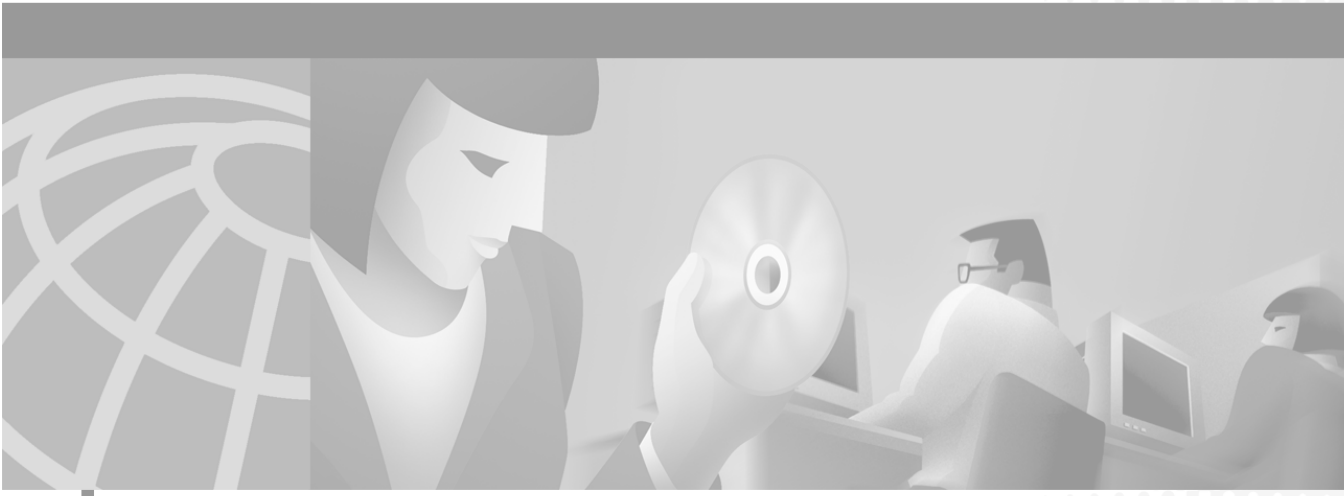
- Introduction, page 1-1
- System Configuration Overview, page 3-1
- Device Support, page 9-1
- Understanding Voice Gateways, page 32-1
- Transcoders, page 18-1
- Conference Bridges, page 17-1

Additional Cisco Documentation

- Cisco CallManager Configuration, *Cisco CallManager Administration Guide*
- Device Defaults Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Gateway Configuration, *Cisco CallManager Administration Guide*
- Transcoder Configuration, *Cisco CallManager Administration Guide*
- Conference Bridge Configuration, *Cisco CallManager Administration Guide*

- *Cisco IP Telephony Network Design Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network
- Cisco IP phones documentation on CCO
  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon
- Gateways documentation on CCO
  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access

Cisco Systems



PART 2

Understanding Cisco CallManager System Configuration

CHAPTER 3

System Configuration Overview

For best results when configuring a complete Cisco IP telephony system, start with the system-level components and work toward the individual devices. For example, you have to configure the appropriate device pools, route patterns, 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 IP telephony network. It covers the following topics:

Basic Configuration Flow

Table 3-1 lists the general steps 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 CallManager software on your servers, and configure the servers as needed for TFTP, database publisher, and database subscriber services.	Refer to *Installing Cisco CallManager Release 3.1* and to the "Server Configuration" section in the *Cisco CallManager Administration Guide*.
Step 2	Configure system-level settings: • Cisco CallManager groups • Date/time groups • Regions • Device pools • Device defaults • Enterprise parameters • Locations	See the "System-Level Configuration Settings" section on page 4-1.
Step 3	Design and configure your dialing plan: • Partitions • Calling search spaces • Route filters • Route groups • Route lists • Route patterns • Translation patterns	See the "Partitions and Calling Search Spaces" section on page 12-1 and the "Understanding Route Plans" section on page 13-1.

Table 3-1 Configuration Overview Checklist (continued)

Configuration Steps		Procedures and related topics
Step 4	Configure media resources: • Conference bridges • Transcoders • Media termination points • Music on hold • Media resource groups • Media resource group lists	See the "Media Resource Management" section on page 16-1. Also refer to the "Media Resource Group Configuration" section in the *Cisco CallManager Administration Guide*.
Step 5	Install and configure one of the following voice messaging systems: • External (non-Cisco) voice messaging system • Cisco Unity voice messaging system • Cisco uOne voice messaging system	See one of the following sections: • "SMDI Voice Mail Integration" section on page 22-1 • "Cisco uOne Voice Messaging Integration" section on page 24-1

Table 3-1 Configuration Overview Checklist (continued)

Configuration Steps		Procedures and related topics
Step 6	Configure system-wide features: • Call park • Call pickup and group call pickup • Cisco IP phone services • Extension mobility • Cisco WebAttendant • Custom phone rings	See the following sections: • "Call Park" section on page 26-1 • "Call Pickup and Group Call Pickup" section on page 27-1 • "Cisco IP Phone Services" section on page 28-1 • "Extension Mobility and Phone Login Features" section on page 29-1 • "Understanding Cisco WebAttendant" section on page 30-1 • "Custom Phone Rings" section on page 31-1
Step 7	Install and configure the gateways.	See the "Understanding Voice Gateways" section on page 32-1.
Step 8	Configure and install the phones; then, associate users with the phones.	See the "Cisco IP Phones" section on page 33-1 and the "Managing User Directory Information" section on page 15-1.
Step 9	Enable computer telephony integration (CTI) application support; then, install and configure the desired CTI applications.	See the "Computer Telephony Integration" section on page 34-1.

Where to Find More Information

Related Topics

- See Table 3-1.

Additional Cisco Documentation

- *Installing Cisco CallManager Release 3.1*
- *Cisco CallManager Administration Guide*

CHAPTER 4

System-Level Configuration Settings

Configure system-wide settings before adding devices and configuring other Cisco CallManager features. This section covers the following topics:

Cisco CallManager Groups

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

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

Cisco 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 CallManager in the group assigned to its device pool. If the primary Cisco CallManager is not available, the device tries to connect to the next Cisco CallManager listed in the group, and so on. Each device pool has one Cisco CallManager group assigned to it.
- Call processing load balancing—You can configure device pools and Cisco CallManager groups to distribute the control of devices across multiple Cisco CallManagers. See the "Balanced Call Processing" section on page 5-5 for more information.

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

Date/Time Groups

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

A default Date/Time Group called CMLocal configures automatically when you install Cisco CallManager. CMLocal synchronizes to the active date and time of the operating system on the Cisco CallManager server. After installing Cisco 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 CallManager or upgrade the Cisco CallManager software to a new release. Do not change the name of CMLocal.

Tips For a worldwide distribution of Cisco IP phones, create one named Date/Time Group for each of the 24 time zones.

You cannot delete a Date/Time Group that any device pool uses. If you try to delete a Date/Time Group that is in use, Cisco CallManager displays an error message. 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 any device pools that are using the Date/Time Group you want to delete.
- Delete the device pools that are using the Date/Time Group you want to delete.

Regions

When you create a region, you specify the voice codec that can be used for calls between devices within that region, and between that region and other regions.

The voice codec type specifies the technology used to compress and decompress voice signals. The choice of voice codec determines the compression type and amount of bandwidth used per call. See Table 4-1 on page 4-5 for specific information about bandwidth usage for available voice codecs.

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

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

To specify voice codec usage for devices using regions, you must:

- Create regions and specify the voice codecs to use for calls within those region and between other regions.
- Create or modify device pools to use the regions you created.
- Assign devices to device pools that specify the appropriate region.

See the "Device Pools" section on page 4-7 for more information about device pool settings.

Supported Voice Codecs and Bandwidth Usage

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

- **G.711**—Default codec for all calls through Cisco CallManager.
- **G.729**—Low-bit-rate codec with 8-kbps compression supported by Cisco IP Phone 7900 Family 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.
- **G.723**—Low-bit-rate codec with 6-kbps compression for older Cisco IP Phone model 12 SP+ and Cisco IP Phone model 30 VIP devices.
- **GSM**—The global system for mobile communications (GSM) codec enables the MNET system for GSM wireless handsets to operate with Cisco CallManager. Assign GSM devices to a device pool that specifies GSM as the voice 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).

Note Cisco IP phones support GSM-FR but not GSM EFR.

- **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 IP Phone 7900 model phones.

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.7ll.

The total bandwidth used per call depends on the voice codec type as well as factors such as data packet size and overhead (packet header size), as indicated in Table 4-1.

Table 4-1 Bandwidth Used per Call by Each Codec Type

Voice 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.723	6 kbps	22 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 CallManager supports wideband audio from IP phone to IP phone for Cisco IP Phone 7900 Family model phones only.
2. Global system for mobile communications.

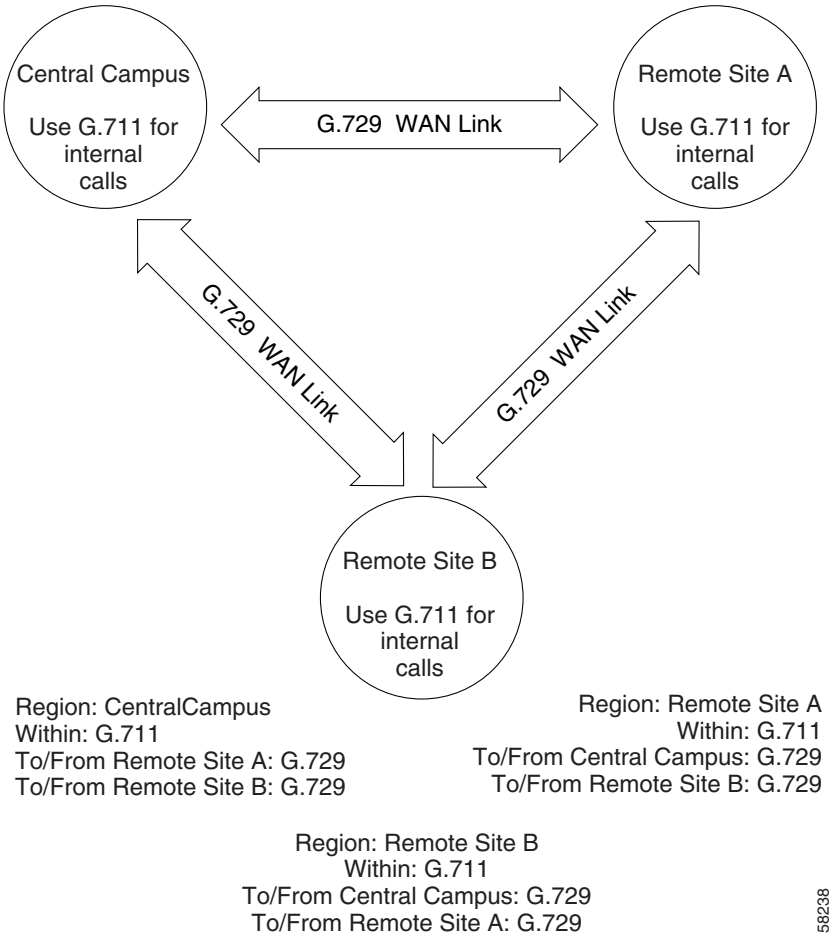
Example

Figure 4-1 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 used for calls within each site, and the G.729 codec equals the maximum bandwidth codec 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 4-1 Simple Region Example



Locations and Regions

In Cisco 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 used on the link (and therefore, the amount of bandwidth used per call), and 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 4-10.

Modifying or Deleting Regions

When you update region settings, the changes do not take effect until you restart the devices that use that region.

You cannot delete a region that any device pool uses. If you try to delete a region that is in use, Cisco CallManager displays an error message. Before deleting a region that is currently in use, you must perform either or both of the following tasks:

- Assign a different region to any device pools that are using the region you want to delete.
- Delete the device pools that are using the region you want to delete.

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:

- Cisco CallManager group—Specifies a prioritized list of up to three Cisco CallManagers to facilitate redundancy. The first Cisco CallManager in the list serves as the primary Cisco CallManager for that group, and the other members of the group serve as secondary (backup) Cisco CallManagers. See the "Cisco CallManager Groups" section on page 4-1 for more details.
- Date/Time group—Specifies the date and time zone for a device. See the "Date/Time Groups" section on page 4-2 for more details.
- Region—Specifies the voice codecs used within and between regions. Use regions only if you have different types of voice codecs within the network. See the "Regions" section on page 4-3 for more details.
- Media resource group list (optional)— Specifies a prioritized list of media resource groups. An application selects the required media resource (for example, a Music On Hold server, transcoder, or conference bridge) from the available media resource groups according to the priority order defined in the media resource group list. See the "Media Resource Group Lists" section on page 16-5 for more details.
- Music On Hold (MOH) audio sources (optional)—Specifies the audio sources for user hold and network hold. See the "Audio Sources for Music On Hold" section on page 19-12 for more details.

- Calling search space for auto-registration (optional) — Specifies the partitions that an auto-registered device can reach when placing a call. See the "Partitions and Calling Search Spaces" section on page 12-1 for more details.
- Auto-Answer Feature Enable — Globally enables or disables the auto-answer feature for all phones in the device pool that support this feature. The auto-answer feature automatically delivers calls to agents who are available and ready to take calls. Agents hear a notification that the call has arrived (for example, a zip tone or a beep tone), but they do not have to press a button to answer the call.

You must configure the preceding items before configuring a device pool if you want to select them for the device pool.

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

To assign all devices of a given type to a device pool, use the Device Defaults page in Cisco CallManager Administration. See the "Device Defaults" section on page 4-9 for more information.

Updating Device Pools

If you make changes to a device pool, you must reset the devices in that device pools 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. If you try to delete a device pool that is in use, an error 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 assigned to the device pool you want to delete.

Device Defaults

Use device defaults to set the system-wide default characteristics of each type of device that registers with a Cisco CallManager. The system-wide device defaults for a device type apply to all devices of that type within a Cisco CallManager cluster. Default settings for devices include

- Device firmware loads
- Device pools
- Phone button templates

When a device registers with a Cisco CallManager, it acquires the system-wide device default settings for its device type. After a device registers, you can update its configuration individually to change the device settings.

Installing Cisco CallManager automatically sets the device defaults. You cannot create new device defaults or delete existing ones, but you can change the default settings.

Before updating the device defaults, perform any of the following tasks that apply to your system:

- Add new firmware files for the devices to the TFTP server. For each available firmware load, a .bin file resides in the Program Files\Cisco\TFTPPath folder on the Cisco CallManager server.

  For example, for the firmware load P002A0305556, a file named P002A0305556.bin resides in the Program Files\Cisco\TFTPPath folder.
- Configure new device pools.
- If the device is a phone, configure new phone templates.

Enterprise Parameters

Enterprise parameters provide default settings that apply to all devices and services in the same cluster. (A cluster is a set of Cisco CallManagers that share the same database.) When you install a new Cisco 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.

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 connecting your main campus and a remote site.

Voice quality can begin to degrade when there are too many active calls 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 on a particular link at the same time. 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 consumed by active calls on the link.

Cisco 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 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 CallManager or Cisco CallManager cluster at each site.

Note If you do not use call admission control to limit the voice bandwidth on an IP WAN link, an unlimited number of calls can 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 7-1 for more information.

System Configuration Checklist

Table 4-2 lists the general steps for configuring system-wide settings.

Table 4-2 System Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Configure Cisco CallManager groups for redundancy.	See the "Cisco CallManager Groups" section on page 4-1. See the "Redundancy" section on page 6-1. Refer to "Cisco CallManager Group Configuration"section in the *Cisco CallManager Administration Guide*.
Step 2	Configure regions, if needed. You do not need to configure regions if you are using only the default G.711 voice codec.	See the "Regions" section on page 4-3. Refer to the "Region Configuration" section in the *Cisco CallManager Administration Guide*.
Step 3	Configure Date/Time groups.	See the "Date/Time Groups" section on page 4-2. Refer to the "Date/Time Group Configuration" section in the *Cisco CallManager Administration Guide*.
Step 4	Configure media resource groups and media resource group lists.	See the "Media Resource Management" section on page 16-1. Refer to the "Media Resource Group Configuration" section in the *Cisco CallManager Administration Guide*.

Table 4-2 System Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 5	Configure device pools.	See the "Device Pools" section on page 4-7. Refer to the "Device Pool Configuration" section in the *Cisco CallManager Administration Guide*.
Step 6	Update device defaults, if needed.	See the "Device Defaults" section on page 4-9. Refer to the "Updating Device Defaults" section in the *Cisco CallManager Administration Guide*.
Step 7	Configure locations or gatekeeper for call admission control.	See the "Locations and Regions" section on page 4-6 and the "Call Admission Control" section on page 7-1.
Step 8	Update enterprise parameters, if necessary.	See the "Enterprise Parameters" section on page 4-9. Refer to the "Enterprise Parameters Configuration" section in the *Cisco CallManager Administration Guide*.

Where to Find More Information

Related Topics

- Cisco CallManager Groups, page 4-1
- Date/Time Groups, page 4-2
- Regions, page 4-3
- Device Pools, page 4-7
- Device Defaults, page 4-9
- Enterprise Parameters, page 4-9
- Call Admission Control, page 4-10
- Redundancy, page 6-1

Additional Cisco Documentation

- *Cisco CallManager Administration Guide*

CHAPTER 5

Clustering

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

This section covers the following topics:

Clusters

A cluster consists of a set of Cisco 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:

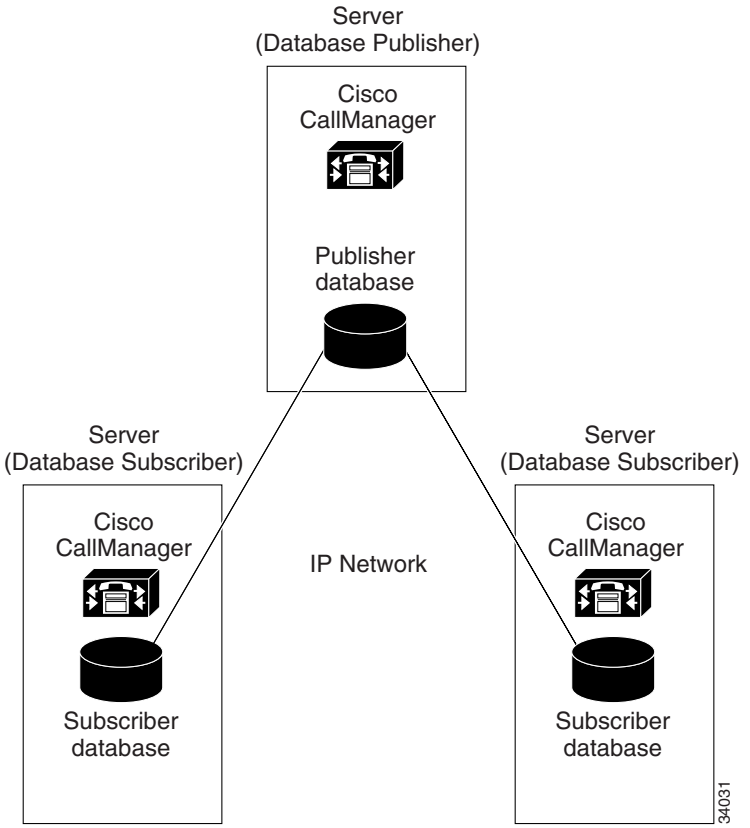
- Database publisher server
- TFTP server
- Application software server
- Primary call-processing server
- Backup call-processing server

When you install the Cisco CallManager software on servers, you specify which servers and which Cisco CallManagers belong to the same cluster. You also 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 you want.

Each cluster can have only one database publisher and one TFTP server (either separate or combined). Other servers in the cluster subscribe to the publisher database maintain their own local copies of it. Figure 5-1 illustrates a simple cluster containing three Cisco CallManagers.

For details on cluster size and recommended configurations, refer to the *Cisco IP Telephony Network Design Guide.*

Figure 5-1 A Cluster with Three Cisco CallManagers



Intracluster Communication

Two primary types of communication occur within a Cisco CallManager cluster. The first type of intracluster communication provides a mechanism for distributing the database that contains all the device configuration information. When you make configuration changes in Cisco CallManager Administration, the publisher server initially stores those changes in its local database. The publisher then sends the new data to all the subscriber servers in the cluster, so that they can update their local copies of the database. This mechanism ensures that the

configuration database remains consistent across all servers in the cluster. It also provides database redundancy because the subscriber servers can continue to operate from their local copies of the database even if the publisher becomes unavailable for any reason.

The second type of intracluster communication involves the propagation and replication of run-time data such as registration of IP phones, gateways, and digital signal processor (DSP) resources. All servers in the cluster share this run-time data, thus ensuring optimum routing of calls between members of the cluster and associated gateways.

Redundancy

Clusters facilitate two types of redundancy in the IP telephony network:

- Database replication
- Device failover and failback

As already mentioned, database redundancy involves the replication of the publisher database across all servers in the cluster. Servers can continue to operate from their own local copies of the database even if they lose communication with the publisher.

The failover and failback mechanism in Cisco CallManager provides call-processing redundancy for devices such as IP phones and gateways. You can configure your system for the level of redundancy you want by using Cisco CallManager groups. A group designates a prioritized list of up to three Cisco CallManagers: a primary, a secondary, and a tertiary. You also configure device pools to assign specific devices to one of the Cisco CallManager groups in a cluster.

During normal operation, each device registers with the primary Cisco CallManager in its assigned group. If the primary Cisco CallManager fails for any reason, all devices in the group failover to the secondary Cisco CallManager for that group. If the secondary Cisco CallManager also fails, the devices failover to the tertiary one. When normal operation resumes, the devices fail back to the primary Cisco CallManager.

You can configure Cisco CallManager groups and device pools in various ways to provide the level of redundancy and load balancing you want in a cluster. For examples and recommendations on redundancy configurations, refer to the *Cisco IP Telephony Network Design Guide.*

Intercluster Communication

In 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 using H.323 protocol. Most large systems use one of three main types of multicluster configurations:

- Large, single campus, or metropolitan-area network (MAN)
- Multisite WAN with distributed call processing (one or more Cisco CallManagers at each site)
- Multisite WAN with centralized call processing (no Cisco CallManager at the remote site or sites)

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. Multisite WANs with centralized call processing can use the locations feature in Cisco CallManager to implement call admission control.

Most features of Cisco 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 IP Telephony Network Design Guide.*

Balanced Call Processing

After installing the Cisco 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 CallManagers in the cluster. To distribute

the devices, you configure Cisco CallManager groups and device pools and then assign the devices to the device pools in a way that achieves the type of load balancing you want.

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

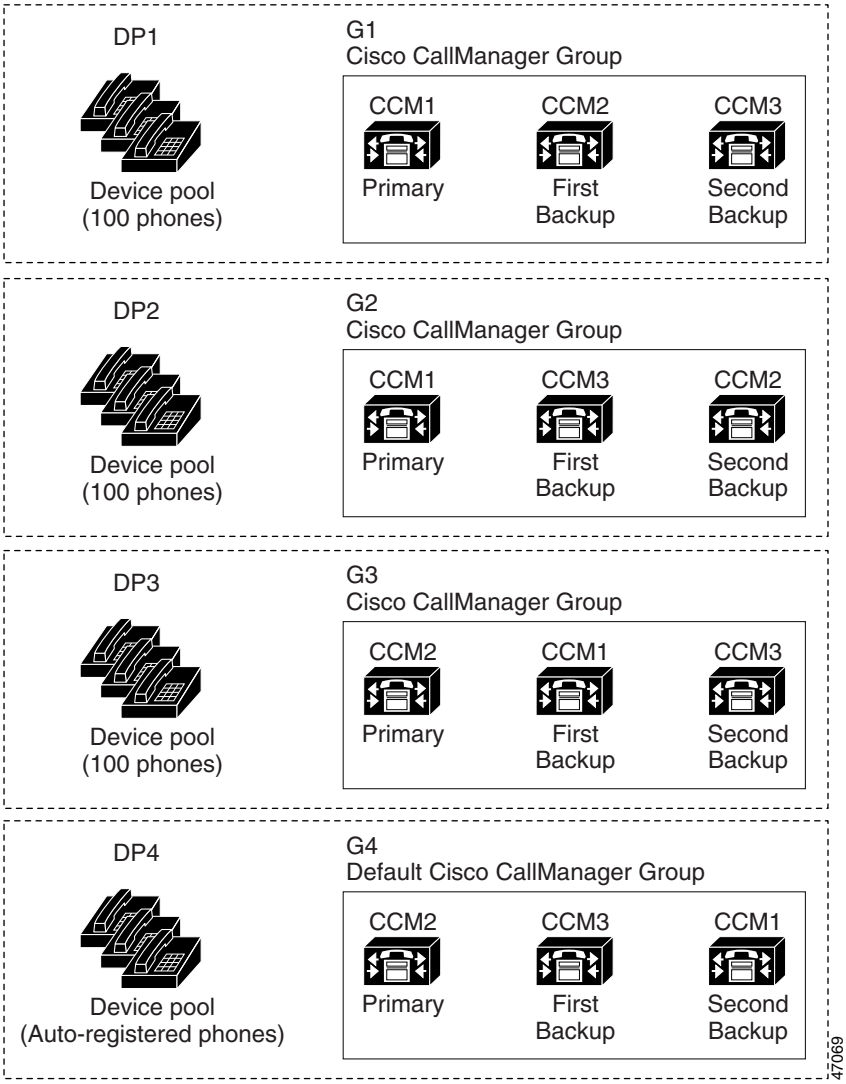
You can also use Cisco CallManager groups to establish redundancy (backup call processors) for the primary Cisco CallManager in the group. A Cisco CallManager group is an ordered list of up to three Cisco CallManager servers. During normal operation, the first (primary) Cisco CallManager in the group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

For example, assume a simplified system consisting of three Cisco CallManagers in a cluster, with 300 existing Cisco IP phones and provisions to auto-register new phones as they are added later. Figure 5-2 shows one possible way to configure the Cisco CallManager groups and device pools to distribute the call processing load for this system.

- The configuration includes four Cisco 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.
- CCM1 serves as the primary Cisco CallManager for the devices in DP1 and DP2, first backup for DP3, and second backup for the devices in DP4.
- CCM2 serves as the primary Cisco CallManager for the devices in DP3 and DP4, first backup for DP1, and second backup for the devices in DP4.
- CCM3 serves as the first backup Cisco CallManager for the devices in DP2 and DP4 and second backup for the devices in DP1 and DP3.

Figure 5-2 represents a balanced system because each Cisco CallManager in the cluster handles only a portion of the call processing load for the entire system. The system in Figure 5-2 also balances redundancy by splitting the call processing load of a primary Cisco CallManager between two redundancy groups. For example, if CCM1 fails, all the devices in device pool DP1 failover to CCM2, and the devices in DP2 failover to CCM3.

Figure 5-2 Cisco CallManager Groups and Device Pools



Cluster Configuration Checklist

Table 5-1 provides an overview of the steps required to install and configure a Cisco CallManager cluster.

Table 5-1 Cluster Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Install the servers and other hardware required for the cluster.	Refer to the installation documentation for the hardware components you are installing.
Step 2	Gather the information you need to install Cisco CallManager and any other software applications on the servers. Also, determine how you will allocate the servers in the cluster.	Refer to • *Cisco IP Telephony Network Design Guide* • *Installing Cisco CallManager Release 3.1* • *Cisco IP IVR Installation Guide*
Step 3	Install Cisco CallManager and any additional software applications on the servers.	Refer to • *Installing Cisco CallManager Release 3.1* • *Cisco IP IVR Installation Guide*
Step 4	Configure Cisco CallManager groups to provide the desired level of redundancy for device failover and failback.	Refer to Cisco CallManager Group Configuration, *Cisco CallManager Administration Guide*.
Step 5	Configure device pools and use them to assign specific devices to a Cisco CallManager group.	Refer to Device Pool Configuration, *Cisco CallManager Administration Guide*.

Table 5-1 Cluster Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 6	If you are using an intercluster trunk, install and configure it as an H.323 device.	Refer to • *Cisco IP Telephony Network Design Guide* • Adding a Cisco IOS H.323 Gateway or Intercluster Trunk, *Cisco CallManager Administration Guide*.
Step 7	If you want to provide call admission control for an intercluster trunk, configure either a gatekeeper or Cisco CallManager locations.	Refer to • *Cisco IP Telephony Network Design Guide* • Gatekeeper Configuration, *Cisco CallManager Administration Guide*. • Location Configuration, *Cisco CallManager Administration Guide*.

Where to Find More Information

Related Topics

- Cisco CallManager Group Configuration, *Cisco CallManager Administration Guide*
- Device Pool Configuration, *Cisco CallManager Administration Guide*
- Adding a Cisco IOS H.323 Gateway or Intercluster Trunk, *Cisco CallManager Administration Guide*
- Gatekeeper Configuration, *Cisco CallManager Administration Guide*
- Location Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Telephone Network Design Guide*
- *Installing Cisco CallManager Release 3.1*
- *Cisco IP IVR Installation Guide*

CHAPTER 6

Redundancy

Cisco CallManager (Release 3.0 and later) provides several forms of redundancy:

- Database redundancy—The Cisco CallManagers in a cluster maintain backup copies of their shared database.
- Call-processing redundancy—Using Cisco CallManager groups, you can designate backup Cisco CallManagers to handle call processing for a disabled Cisco CallManager in a form of redundancy known as device failover.
- Media resource redundancy
- CTI redundancy

This section covers the following topics:

Cisco CallManager Redundancy Groups

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

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

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

Cisco CallManager Groups

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

Cisco CallManager groups provide both redundancy and recovery:

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

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

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

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

You associate devices with a Cisco CallManager group by using device pools. You can assign each device to one device pool and associate each device pool with one Cisco CallManager group. You can combine the groups and device pools in various ways to achieve the desired level of redundancy. For example, Figure 6-1 shows a simple system with three Cisco CallManagers in a single group controlling 800 devices.

Figure 6-1 Cisco CallManager Group

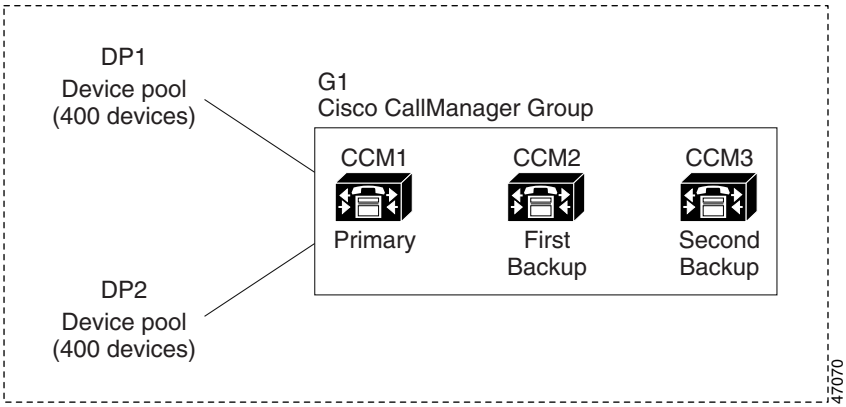


Figure 6-1 depicts Cisco CallManager group G1 assigned with two device pools, DP1 and DP2. CCM1, as the primary Cisco CallManager in group G1, controls all 800 devices in DP1 and DP2 under normal operation. If CCM1 fails, control of all 800 devices transfers to CCM2. If CCM2 also fails, control of all 800 devices transfers to CCM3.

The configuration in Figure 6-1 provides call processing redundancy, but it does not distribute the call processing load very well among the three Cisco CallManagers in the example. For information on load balancing, see the "Distributing Devices for Redundancy and Load Balancing" section on page 6-4.

Distributing Devices for Redundancy and Load Balancing

Cisco CallManager groups provide both call processing redundancy and distributed call processing. How you distribute devices, device pools, and Cisco 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 CallManagers from becoming overloaded if one Cisco CallManager in the group fails. Figure 6-2 shows one possible way to configure the Cisco CallManager groups and device pools to achieve both distributed call processing and redundancy for a system of three Cisco CallManagers and 800 devices.

Figure 6-2 Redundancy Combined with Distributed Call Processing

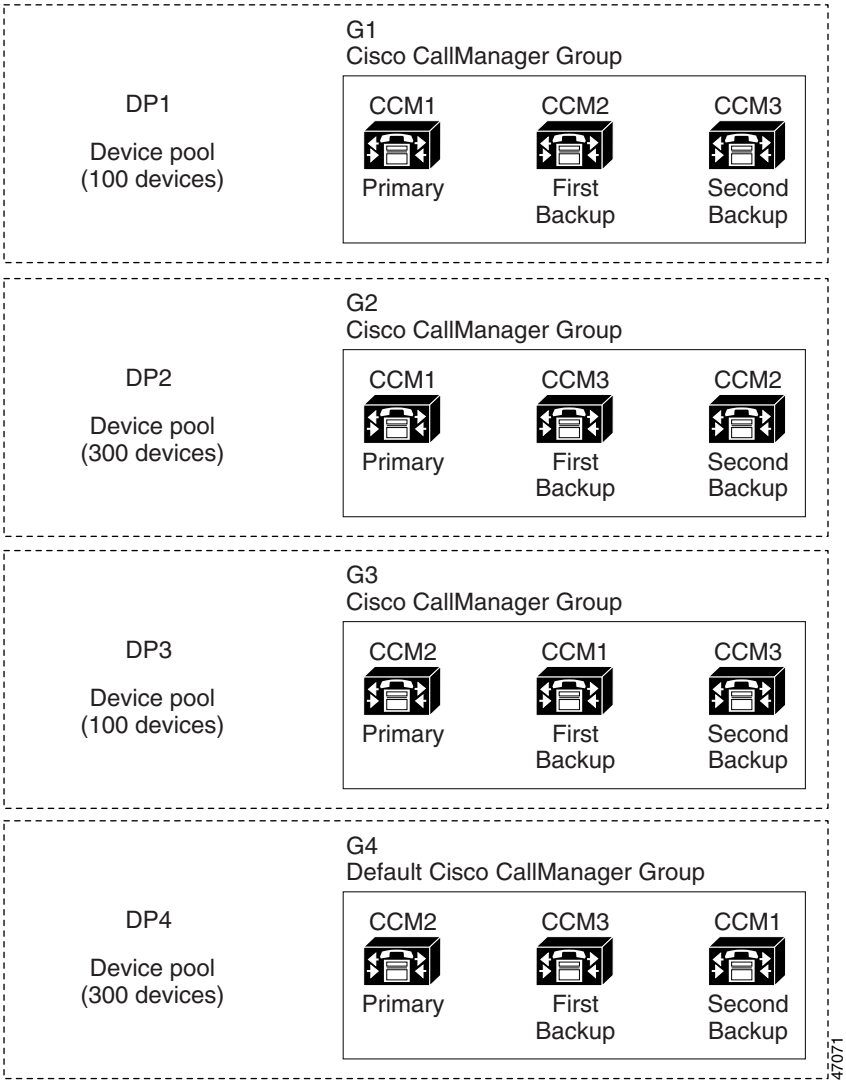


Figure 6-2 depicts the Cisco CallManager groups configured and assigned to device pools, so that Cisco CallManager CCM1 is the primary controller in two groups, G1 and G2. If CCM1 fails, the 100 devices in device pool DP1 reregister

with CCM2, and the 300 devices in DP2 reregister with CCM3. Similarly, CCM2 serves as the primary controller of groups G3 and G4. If CCM2 fails, the 100 devices in DP3 reregister with CCM1, and the 300 devices in DP4 reregister with CCM3. If CCM1 and CCM2 both fail, all devices reregister with CCM3.

For more information on distributed call processing, see the "Balanced Call Processing" section on page 5-5.

Database Redundancy

When you make configuration changes in Cisco CallManager Administration, the publisher server initially stores those changes in its local database. The publisher then sends the new data to all the subscriber servers in the cluster, so that they can update their local copies of the database. This mechanism ensures consistency of the configuration database across all servers in the cluster. It also provides database redundancy because the subscriber servers can continue to operate from their read-only local copies of the database even if the publisher becomes unavailable for any reason.

Database redundancy also provides for the propagation and replication of run-time data such as registration of IP phones, gateways, and digital signal processor (DSP) resources. All servers in the cluster share this run-time data, thus ensuring optimum routing of calls between members of the cluster and associated gateways.

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 defined in the media resource list. For more information on media resource redundancy, see the "Media Resource Management" section on page 16-1.

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 CallManager
- CTI Manager
- Applications that use CTI

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

Where to Find More Information

Related Topics

- Clustering, page 5-1
- Media Resource Management, page 16-1

Additional Cisco Documentation

- *Cisco IP Telephony Network Design Guide*

CHAPTER 7

Call Admission Control

Call admission control enables you to control the audio quality of calls over a wide-area (IP WAN) link by limiting the number of calls 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 connecting your main campus and a remote site.

Audio quality can begin to degrade when there are too many active calls on a link and the amount of bandwidth is oversubscribed. Call admission control regulates audio 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 quality on the link, but it does allow you to regulate the amount of bandwidth consumed by active calls on the link.

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

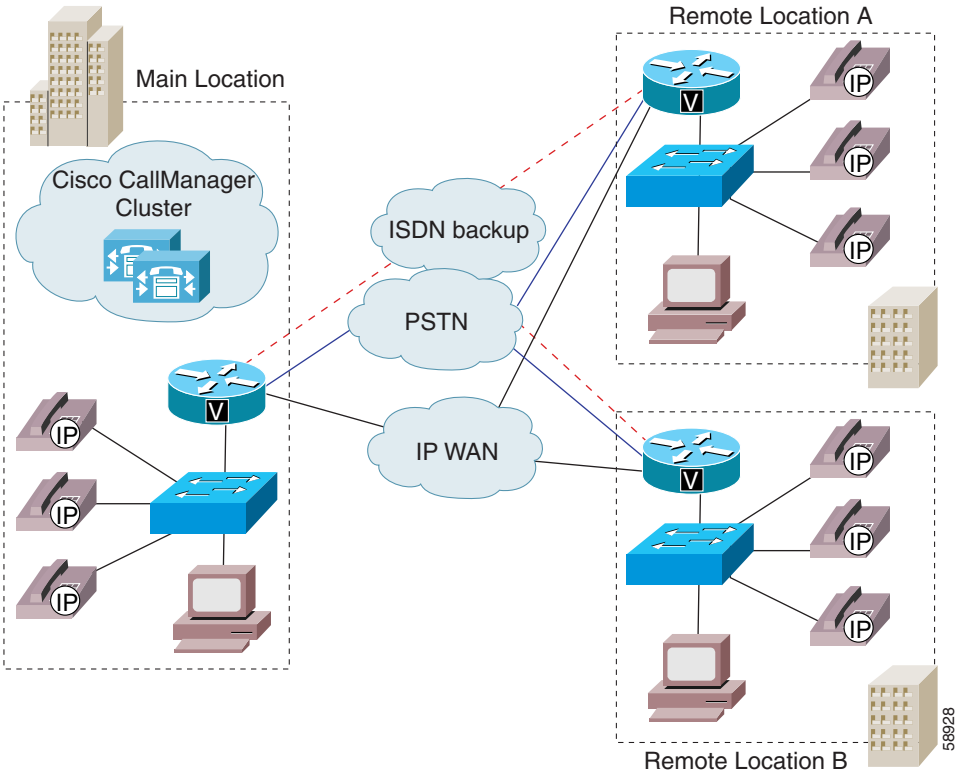
- Locations, page 7-2, for systems with centralized call processing
- Gatekeeper, page 7-8, for systems with distributed call processing

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

Locations

The locations feature, available in Cisco CallManager, provides call admission control for centralized call processing systems. A centralized system uses a single Cisco CallManager cluster to control all the locations. Figure 7-1 illustrates call admission control using locations. For more information, refer to the "Location Configuration" section in the *Cisco CallManager Administration Guide* and to the *Cisco IP Telephony Network Design Guide*.

Figure 7-1 Call Admission Control Using Locations in a Centralized System



In a centralized call processing system, as illustrated in Figure 7-1, the Cisco 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 and to each other by means of IP WAN links (and possibly PSTN and ISDN links as backups).

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 CallManager lets you specify the maximum amount of bandwidth available for calls to and from each location, thereby limiting the number of active calls and preventing oversubscription of the bandwidth on the IP WAN links.

For location bandwidth calculations, Cisco CallManager assumes that each call consumes the following amount of bandwidth:

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

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

Location	Bandwidth (kbps)
San Francisco (main location)	Unlimited
Austin (remote location)	100
Dallas (remote location)	200

Cisco 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 our example has 100 kbps of available bandwidth, that link can support one G.711 call at 80 kbps, four G.723 or G.729 calls at 24 kbps each, or three GSM calls at 29 kbps

each. 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.

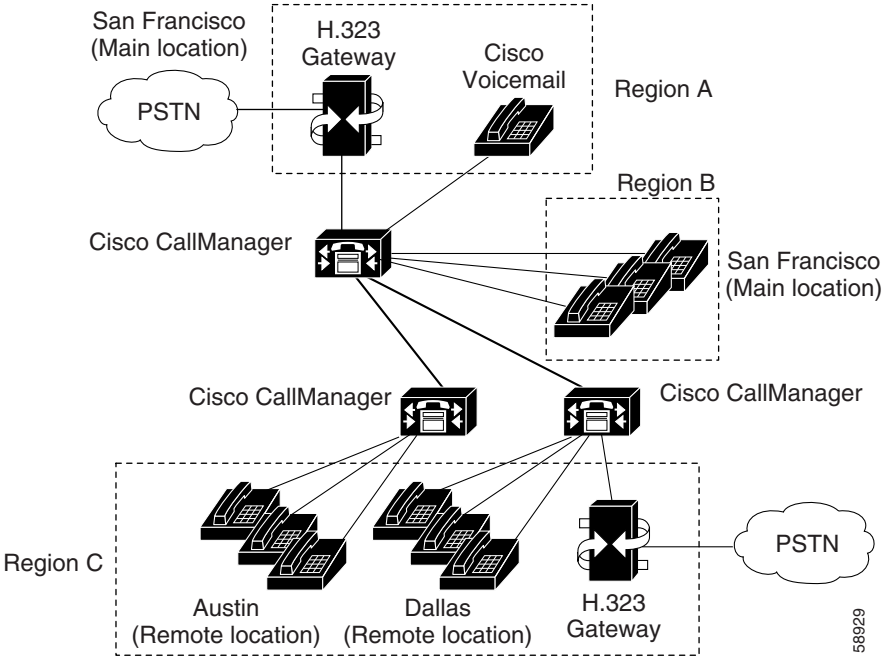
When you configure a location in Cisco CallManager Administration, you assign it a name and maximum bandwidth. If you enter a value of zero (0) for the bandwidth, you allocate unlimited available bandwidth and allow an unlimited number of active calls on the IP WAN link for that location.

When you configure a phone or other device in Cisco CallManager Administration, you can assign it to a location. If you set the location to *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.

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.723, or G.729) used on the link, and locations define the amount of available bandwidth for the link. You must assign each device in the system to both a region (by means of a device pool) and a location. As illustrated in Figure 7-2, 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 4-3.

Figure 7-2 Interaction Between Locations and Regions



Bandwidth Calculations

In performing bandwidth calculations for purposes of call admission control, Cisco CallManager assumes that all calls are full-duplex connections. Cisco CallManager also assumes that each call consumes the following amount of bandwidth:

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

Note Actual bandwidth consumption per call will vary, depending on factors such as data packet size. Cisco CallManager uses these fixed values to simplify the bandwidth calculations for purposes of the locations feature only.

Cisco CallManager allows calls to complete over a link until there is no longer sufficient bandwidth for a new call. At that point, any additional calls fail and the calling party receives reorder tone.

A Media Termination Point (MTP) is one exception to the bandwidth rules outlined in the preceding paragraph. Calls made through an MTP can complete even if they exceed the available bandwidth limit.

Caution In the United States and Canada, routing an emergency 911 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.

Locations Configuration Checklist

Table 7-1 lists the general steps for configuring call admission control based on locations.

Table 7-1 Locations Configuration Checklist

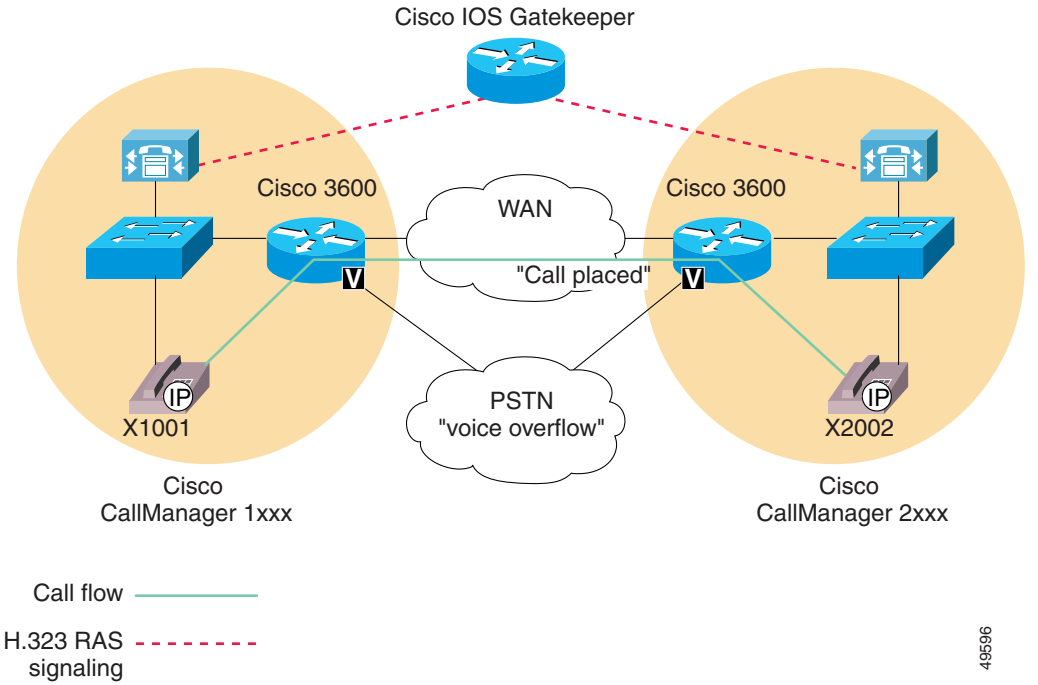
Configuration Steps		Procedures and Related Topics
Step 1	Configure a region for each type of codec used in your system.	See the "Locations and Regions" section on page 7-4. Refer to the "Region Configuration" section in *Cisco CallManager Administration Guide*.
Step 2	Configure a separate location for 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 enter a value of zero (0) for the bandwidth, you allocate unlimited available bandwidth and allow an unlimited number of active calls on the IP WAN link for that location.	Refer to the "Location Configuration" section in the *Cisco CallManager Administration Guide*.
Step 3	Configure the device pools for your system and select the appropriate region for each.	Refer to the "Device Pool Configuration" section in the *Cisco 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 *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.	See the "Cisco IP Phones" section on page 33-1. Refer to the "Cisco IP Phone Configuration" section in the *Cisco CallManager Administration Guide*.

Gatekeeper

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 7-3 shows two sites, each with its own Cisco CallManager, connected by and IP WAN link. The gatekeeper provides call admission control over the IP WAN link in this example.

In addition to call admission control, the gatekeeper can also perform E.164 address resolution to route calls between the sites. For example, in Figure 7-3, one Cisco CallManager has an extension range of 1XXX and the other 2XXX. Both register with the gatekeeper for call admission control. Each Cisco CallManager has an appropriate entry in its respective dial plan route pattern configuration that points the other Cisco CallManager extension number range to the gatekeeper. In practice, when user 1001 dials user 2002, Cisco 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 CallManager 2XXX to Cisco CallManager 1XXX. Using the IP address of Cisco CallManager 2XXX, Cisco CallManager 1XXX can then complete the call to directory number 2002.

Figure 7-3 Call Admission Control Using a Gatekeeper in a Distributed System



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 (Anonymous Calls Device) for address resolution. If the gatekeeper does not allow the call to go over the WAN, then Cisco CallManager can add the prefix 91 to the dialed digits to reroute the call through the PSTN.

Refer to the *Cisco IP Telephony Network Design Guide* for more detailed information about gatekeeper configuration, dial plan considerations when using a gatekeeper, and gatekeeper interaction with Cisco CallManager.

Components of Gatekeeper Call Admission Control

Gatekeeper call admission control is very flexible:

- The gatekeeper reduces configuration overhead by eliminating the need to configure a separate H.323 device for each remote Cisco CallManager connected to the IP WAN.
- The gatekeeper can determine the IP addresses of devices registered with it, or you can enter the IP addresses explicitly.
- The gatekeeper offers a choice of protocols for communicating with Cisco CallManagers or H.225 gateways.
- The gatekeeper can perform basic call routing in addition to call admission control.
- You can connect up to 100 Cisco CallManager clusters to a single gatekeeper.

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

- Gatekeeper Configuration on the Router, page 7-10
- Gatekeeper Configuration in Cisco CallManager, page 7-12

Gatekeeper Configuration on the Router

Recommended platforms for the gatekeeper include Cisco 2600, 3600, 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. Each zone has a unique name and includes the IP address of each Cisco CallManager that registers with that zone, the zone prefix (directory number range), and the bandwidth allocated for that zone.

Cisco CallManager registers with the gatekeeper 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 CallManager IP address explicitly.
- Enter a **1#*** in the Technology Prefix field under **Device > Gatekeeper** in Cisco CallManager Administration, and enter the command **gw-type-prefix 1#* default-technology** on the gatekeeper. When a Cisco CallManager

registers with the gatekeeper, it sends its IP address and the specified technology prefix to the gatekeeper. The gatekeeper then registers this Cisco CallManager as a valid gatekeeper-controlled VoIP device.

You can associate the Cisco CallManager IP address with a particular zone in one of the following ways:

- Use the **zone subnet** command on the gatekeeper to associate each IP address explicitly with a zone.
- Enter the zone name in the Zone field under **Device > Gatekeeper** in Cisco CallManager Administration. When a Cisco CallManager registers with the gatekeeper, it sends its IP address and the specified zone name to the gatekeeper. The gatekeeper then registers each Cisco CallManager and associates it with the appropriate zone.

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

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

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

```
zone bw 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 Cisco Multimedia Conference Manager documentation.

Gatekeeper Configuration in Cisco CallManager

You can configure the gatekeeper in Cisco CallManager administration to function in either of the following ways.

Call Admission Control Only

In this case, you explicitly configure a separate intercluster trunk or H.225 gateway for each remote device that the local Cisco 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 or H.225 gateways. The intercluster trunks and H.225 gateways statically specify the IP addresses of the remote devices. Use this method only for small systems, where the number of remote connections is minimal. To select this method, uncheck the Allow Anonymous Calls check box under **Device > Gatekeeper**.

Call Admission Control Plus IP Address Resolution (Call Routing)

In this case, you configure only the gatekeeper settings in Cisco CallManager and not the intercluster trunks or H.225 gateways. You also configure route patterns or route groups to route the calls to and from the gatekeeper, but this method generally requires fewer route patterns than when you use intercluster trunks or H.225 gateways. 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 CallManager uses that IP address to complete the call. Use this method for large systems or small ones as well. To select this method, check the Allow Anonymous Calls check box under **Device > Gatekeeper**.

If you enable the Allow Anonymous Calls option, Cisco CallManager automatically creates a virtual device called AnonymousDevice. The IP address of this AnonymousDevice changes dynamically to reflect the IP address of the remote device as determined by the gatekeeper. Use the AnonymousDevice when configuring the route patterns or route groups that route calls to and from the gatekeeper.

Gatekeeper Configuration Checklist

Table 7-2 lists the general steps for configuring call admission control based on a gatekeeper.

Table 7-2 Gatekeeper 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 CallManagers that will route calls to it.	Refer to your Cisco Multimedia Conference Manager documentation.
Step 2	Configure the gatekeeper settings in Cisco CallManager Administration. If you enable the Allow Anonymous Calls option, skip Step 3. Repeat this step for each Cisco CallManager that will register with the gatekeeper. Make sure Gatekeeper Name and Allow Anonymous Calls are set the same way on each Cisco CallManager.	Refer to the "Gatekeeper Configuration" section in the *Cisco CallManager Administration Guide*.
Step 3	If you did not enable the Allow Anonymous Calls option, configure the appropriate intercluster trunks or H.225 gateways to specify the IP addresses of the remote devices registered with the gatekeeper.	See the "H.323 Gateways" section on page 32-6. Refer to the "Adding a Cisco IOS H.323 Gateway or Intercluster Trunk" section in the *Cisco CallManager Administration Guide*.
Step 4	Configure a route pattern to route calls to the gatekeeper.	See the "Understanding Route Plans" section on page 13-1. Refer to the "Route Pattern Configuration" section in the *Cisco CallManager Administration Guide*.

Where to Find More Information

Related Topics

- Location Configuration, *Cisco CallManager Administration Guide*
- Region Configuration, *Cisco CallManager Administration Guide*
- Gatekeeper Configuration, *Cisco CallManager Administration Guide*
- Gateway Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Telephony Network Design Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network/
- Cisco Multimedia Conference Manager (Command Reference) IOS documentation

CHAPTER 8

Cisco TFTP

The Cisco TFTP service builds and serves files consistent with the trivial file transfer protocol, which is a simplified version of the File Transfer Protocol (FTP). 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 CallManagers for a device (telephones and gateways), the TCP port on which the device connects to those Cisco CallManagers, and an executable load identifier. Configuration files for Cisco IP Phone 7960 and 7940 models also contain 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 format or a .cnf.xml format, depending on the device type and your TFTP service parameter settings. When you set the BuildCNFFlag service parameter to True, the TFTP server builds both .cnf.xml and .cnf format configuration files for devices. When you set the parameter to False, the TFTP server builds only .cnf.xml files for devices.

This section describes the relationship among Cisco 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

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.

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 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 CallManager name, it resolves the name using DNS and opens a Cisco 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 requesting a configuration file while the TFTP server is processing the maximum number of requests (30) receive an error message from the TFTP server, which causes the device to request the configuration file later.

For a more detailed description of how devices boot, see the "Understanding How Devices Use DHCP and Cisco TFTP" section on page 8-3.

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. For example, you can connect multiple Cisco 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 IP phones are 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 is 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 IOS command-line interface on the Cisco Catalyst 6000.

Requesting the Configuration File

Once 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 CallManager database, the device accesses a configuration file corresponding to its device name. If auto-registration is enabled in Cisco CallManager, the phones access a default configuration file from the TFTP server.

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 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 The TFTP server only builds the .cnf format configuration files if you leave the BuildCNFFlag service parameter set to the default value of True. You must leave this parameter set to the default value until you have converted all of your phones to the Cisco CallManager 3.1 release. You must continue to use the default value if you are using third party phones.

Contacting Cisco CallManager

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

Cisco CallManager informs devices using .cnf format configuration files of their load ID. Devices 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 associated with the new load ID from the TFTP server and resets itself. For more information on device loads, see the "Device Support" section on page 9-1.

Once 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 DNS Host Name or IP address of the TFTP server as the option value.

- Gateways and phones can query CiscoCM1.

  The Domain Name System (DNS) must be able to resolve this name to the IP address of the TFTP server.

- 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 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 saved in memory.

The TFTP server must subscribe to the Cisco CallManager publisher (master database). For small systems, the TFTP server can coexist with a Cisco CallManager on the same server.

Understanding How Devices Identify the TFTP Server

Phones and gateways have an order of precedence that they use 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 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 sent by the DHCP server.

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 sent by the DHCP server.

   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.

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 configuring BOOTP servers, this field typically serves as the address of the TFTP server.

   This information is 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 DNS name of a TFTP server. Currently, you can configure only a DNS 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 DNS name or a dotted decimal IP address.

   Do not use the 066 option with the 150 option.

   If they are sent together, the device prefers the IP address over the name given by the 066 option. However, 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. To reiterate, option 066 and option 150 are mutually exclusive.

Alternate TFTP Paths

You can specify alternate TFTP paths if you have multiple clusters. You only want to configure one server for many DHCP scopes. The TFTP server stores files for the cluster containing the TFTP server in the primary path and stores the files for the other clusters in alternate paths. You can specify up to 10 alternate paths by entering a value for the AlternateFileLocation parameters. For more information on TFTP service parameters, refer to the "Service Parameters Configuration" in the *Cisco CallManager Administration Guide*.

TFTP Configuration Checklist

Table 8-1 lists the steps needed to configure the Cisco TFTP service.

Table 8-1 TFTP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Install the TFTP service on the appropriate server.	Inserting Cisco TFTP Service on a Server, *Cisco CallManager Administration Guide*
Step 2	Configure the appropriate service parameters, including the AlternateFileLocation parameters, if appropriate.	Updating a Service Parameter, *Cisco CallManager Administration Guide*

Where to Find More Information

Related Topics

- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- Cisco TFTP Configuration, *Cisco CallManager Administration Guide*

CHAPTER 9

Device Support

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

Supported Devices

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

- Cisco IP phones
- Analog gateway ports
- T1 gateway
- E1 gateway
- Transcoding resource
- Software Media Termination Point (MTP)
- Conference resource (hardware)

- Conference resource (software)
- CTI port (TAPI and JTAPI)
- Cisco SoftPhone
- Messaging (voice mail)
- Intercluster trunk

Device Configuration Files

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

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

- SEP—Selsius Ethernet Phone (Cisco IP Phone model 12 SP+, Cisco IP Phone model 30 VIP, Cisco IP Phone 7910, Cisco IP Phone 7940, and Cisco IP Phone 7960)
- SAA—Selsius Analog Access (AT-2, 4, 8 and AS-2, 4, 8, and 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)
- MTP—Media Termination Point

Configuration files also contain a list of Cisco 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 8-1 for more information.

When a device has a communication request record that needs to download a configuration file, the following list describes the process used by a device to get to the configuration file:

- A device specifies a device pool.
- A device pool specifies a Cisco CallManager group.

- A Cisco CallManager group specifies a list of Cisco CallManagers.
- Cisco CallManagers contain the TCP connection port for the three device types (IP phone, analog gateway, and digital gateway).

Note If the device is a Cisco IP Phone 7960, you can specify button URLs in device configuration. If the URL is blank, Cisco CallManager uses the enterprise values. Refer to Enterprise Parameters Configuration, in the *Cisco 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 CallManager provides the latest loads. However, you can also receive a load between releases that can contain patches or other information important to the devices that use loads, such as phones or gateways.

The Cisco\TFTPPath subdirectory stores these load files as *.bin 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.

Table 9-1 describes the loads for each device type.

Table 9-1 Device Load Descriptions

Device	Description
Cisco IP Phone models 12S, 12SP, 12SP+, and 30VIP	Loads for these devices begin with P002...; for example, P002K202.
Cisco IP Phone model 30SP+	Loads for these devices begin with P001...; and are 12 characters.
Cisco IP Phone 7960, 7940	Loads for these devices begin with P003...; and are 12 characters.
Cisco IP Phone 7910	Loads for these devices begin with P004...; and are 12 characters.

Table 9-1 Device Load Descriptions (continued)

Device	Description
Cisco IP Conference Station 7935	Loads for these devices begin with P005...; and are 12 characters.
14-Button Line Extension Module	Loads for these devices begin with S001...; and are 12 characters.
Cisco Access Analog gateway	Loads for these devices begin with A001...; and are 12 characters.
Cisco Access Digital gateway	Loads for these devices begin with D001...; and are 12 characters.
Cisco Access Digital + gateway	Loads for these devices begin with D003...; and are 12 characters.
Cisco Voice Gateway 200	Not applicable.
Cisco Catalyst 6000 8 Port T1/E1 and Services Module	Loads for these devices vary depending on how the device is being used: • Conference bridge loads begin with C001. • Digital gateway loads begin with D004. • Transcoder loads begin with M001. These loads are 12 characters.
Cisco Catalyst 6000 24 Port FXS Analog Interface Module	Loads for these devices begin with A002...; and are 12 characters.

Updating Device Loads

You can apply a new load to a single device before applying it as a system-wide default. This method can prove useful for testing purposes. Remember, however, that only the device 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 system-wide defaults for that device with the new load.

Device Pools

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

- Cisco CallManager group—This group specifies a list of up to three Cisco 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 used within and between regions.

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 restricted only to the Cisco CallManager administrator. This search space can have a Primary Line Automatic Ringdown assigned to it, so, when the user goes off hook, the call immediately connects to security or the Cisco 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 used:

- Single-site cluster no WAN voice interconnectivity—Device pool configuration uses only Cisco CallManager redundancy groups as basis: typically, this includes a maximum of four device pools assuming six Cisco CallManagers A, B, C, D, E, and F with the redundancy groups AEF, BEF, CFE, and DFE. The scenario does not require use of regions as all calls use the G.711 codec for calls.
- Multisite WAN centralized call processing—In this case only a single Cisco CallManager redundancy group exists; however, each location requires a G.711 and G.729 region to permit intrabranch calls to be placed as G.711 and interbranch calls to be placed as G.729, for example.
- Multisite WAN distributed call processing—Device pools configured as in preceding scenario also include the additional complexity of regions for codec selection. Each cluster could potentially have a G.711 and G.729 region per Cisco CallManager redundancy group.

- Total device pools = number of sites x regions.

  Total device pools = regions x Cisco CallManager redundancy groups.

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

Call Preservation

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

Beginning with Release 3.1, Cisco CallManager supports full call preservation for an extended set of Cisco IP telephony devices. Limited call preservation support existed for the Cisco CallManger 3.0 and 3.0(5) releases. This support includes call preservation between Cisco IP phones, Media Gateway Control Protocol (MGCP) gateways supporting 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 are connected through one of the following devices, Cisco CallManager maintains call preservation:

- Cisco 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 uOne voice-mail application
- Cisco WebAttendant

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

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

Call Preservation Scenarios

Table 9-2 lists and describes how call preservation is handled in various scenarios.

Table 9-2 Call Preservation Scenarios

Scenario	Call Preservation Handling
Cisco CallManager fails	A Cisco CallManager failure causes the call-processing function for all calls that were set up through the failed Cisco CallManager to be lost. The affected devices recognize that their current Cisco CallManager failed. Similarly, the other Cisco CallManagers in the cluster detect the Cisco CallManager failure. Cisco 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 maintained as a result of this failure.
Communication failure between Cisco CallManager and device	When communication fails between a device and the Cisco CallManager that controls it, the device recognizes the failure and maintains active connections. The Cisco CallManager recognizes the communication failure and clears call-processing entities that are associated with calls in the device where communication was lost. However, the Cisco CallManagers still maintain control of the surviving devices associated with the affected calls. Cisco 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 maintained as a result of this failure.

Table 9-2 Call Preservation Scenarios (continued)

Scenario	Call Preservation Handling
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 CallManager recognizes the device failure and clears call-processing entities that are associated calls in the failed device. However, the Cisco CallManagers maintain control of the surviving devices associated with the affected calls. Cisco CallManager maintains the active connections (calls) 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.
WebAttendant	Call preservation does not apply for Computer Telephony Integration (CTI) route point devices because a call is only accepted for redirect. If a Cisco CallManager goes down before the call is extended to Telephony Call Dispatcher (TCD), the call does not transfer to TCD. If the Cisco CallManager goes down before the call arrives at a phone after TCD redirects the call, the call will be lost. Cisco WebAttendant client inherits call preservation from the phone because it is a third-party control for a phone. Any active calls continue after Cisco CallManager goes down, but calls on hold do not. Cisco WebAttendant only supports call preservation via the associated phone.

Where to Find More Information

Related Topics

- Cisco TFTP, page 8-1
- Understanding Voice Gateways, page 32-1
- Cisco IP Phones, page 33-1

Additional Cisco Documentation

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

CHAPTER 10

Services

Cisco provides several Windows services that you install when you install the Cisco CallManager. Once you install the services, you can configure the service by modifying the service parameters. For more information about service parameters, refer to the Service Parameters Configuration section in the *Cisco CallManager Administration Guide*.

This section provides a description of the available services:

Cisco CallManager

The Cisco CallManager service runs on the Cisco IP Telephony Applications Server to provide software-only call processing as well as signaling and call control functionality. You install the Cisco CallManager service from the Cisco CallManager CD by checking the Cisco CallManager check box on the CallManager Components window.

After you install the service, you configure your Cisco CallManager by modifying the service parameters on the Service Parameters Configuration pane of the Cisco CallManager Administration. Cisco provides over 100 service parameters for the Cisco CallManager service. To view a list of parameters and their descriptions, click the "i" button in the upper, right corner of the Service Parameters Configuration pane. To view the list with a particular parameter at the top, click that parameter on the pane.

You must restart Cisco CallManager after making certain changes in the Cisco CallManager Administration. Table 10-1 lists the changes requiring a restart.

Table 10-1 Restart Conditions

Field Description	Path to This Parameter in Cisco CallManager Administration
IP address of the Cisco CallManager server	System > Server
Partition for auto-registration	System > Cisco CallManager
External phone number mask for auto-registration	System > Cisco CallManager
TCP port settings for the Cisco CallManager server	System > Cisco CallManager

Tips

In general, make as many configuration changes as possible at one time and restart Cisco CallManager only once after completing the changes.

Cisco TFTP

Cisco Trivial File Transfer Protocol (TFTP) builds and serves files consistent with the trivial file transfer protocol, a simplified version of FTP. Cisco TFTP serves embedded component executable, ringer files, and device configuration files.

A configuration file includes a list of Cisco CallManagers to which devices (telephones and gateways) make connections. When a device boots, the component queries a Dynamic Host Configuration Protocol (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.

The device requests a configuration file from the TFTP server. The configuration file contains a list of Cisco CallManagers and the TCP port through which the device connects to those Cisco CallManagers. Cisco IP Phone 7960 and 7940 models, the configuration file also contains phone button URL information.

If the device receives the Cisco CallManager name, the device resolves the name using DNS, and a Cisco CallManager connection is opened. If the device does not receive either an IP address or name, the device uses the default server name.

For more information about TFTP, see the "Cisco TFTP" section on page 8-1.

Cisco Database Layer Monitor

The Cisco Database Layer Monitor service monitors aspects of the database layer as well as call detail records (CDRs). The database layer comprises a set of dynamic link libraries (DLLs) that provide a common access point for applications that need to access the database to add, retrieve, and change data. The Cisco Database Layer Monitor service performs functions such as determining whether the primary server is available during failover, deleting the oldest CDRs when the limit defined in the MaxCDRecords parameter is reached, and moving CDRs from a subscriber to the primary database at a given interval, if needed.

Cisco Messaging Interface

The Cisco Messaging Interface allows you to connect a simplified message desk interface (SMDI)-compliant external voice-mail system with the Cisco CallManager. The CMI service provides the communication between the voice-mail system and Cisco CallManager. The SMDI defines a way for a phone system to provide a voice-mail system with the information needed to intelligently process incoming calls.

You configure the CMI service parameters to define aspects of the CMI service, including

- The serial port connection that CMI uses to communicate with the voice-mail system
- The voice-mail directory number
- The name of the primary and backup Cisco CallManager

For more a general description of how to integrate an SMDI-compliant voice-mail system with Cisco CallManager, see the "SMDI Voice Mail Integration" section on page 22-1.

Cisco IP Voice Media Streaming App

The Cisco IP Voice Media Streaming Application provides voice media streaming functionality for the Cisco CallManager for use with MTP, conferencing, and music on hold (MOH). The Cisco IP Voice Media Streaming Application relays messages from the Cisco CallManager to the IP voice media streaming driver. The driver handles the RTP streaming. The MTP and conference bridge components of the Cisco IP Voice Media Streaming Application support G.711 mu-law and a-law codecs. The MOH component supports G.711 mu-law/a-law, G.729a, and wideband codecs.

When you install the Cisco IP Voice Media Streaming Application, Cisco CallManager automatically installs the Cisco MOH Audio Translator service. For more information about this service, see the "Cisco MOH Audio Translator" section on page 10-6.

You can install the Cisco IP Voice Media Stream application from the Cisco CallManager CD or from the Cisco Service Configuration utility. During installation, Cisco CallManager automatically adds the MTP, MOH, and conference devices to the database. By default, the installation program places the executable in the C:\Program Files\Cisco\bin directory.

Note You can also install the Cisco IP Voice Media Streaming application from a command line by entering *ipvmsapp -Service*. If you do this, you must manually add the MTP, MOH, and conference bridge devices.

For more information about MTP, MOH, and conference bridges, see the "Media Termination Points" section on page 20-1, the "Music On Hold" section on page 19-1, and the "Conference Bridges" section on page 17-1.

Cisco Telephony Call Dispatcher

Telephony Call Dispatcher (TCD) service provides centralized services for Cisco WebAttendant clients and pilot points. For Cisco WebAttendant clients, TCD provides call control functionality, line state information for any accessible line within the Cisco CallManager domain, and caching of directory information. For pilot points, TCD provides automatic redirection to directory numbers listed in hunt groups and failover during a Cisco CallManager failure.

For more detailed information on how TCD works with Cisco WebAttendant clients, see the "Understanding the Cisco Telephony Call Dispatcher" section on page 30-5.

For more information on how TCD works with pilot points, see the "Understanding Pilot Points and Hunt Groups" section on page 30-8.

Cisco CTIManager

The CTI Manager contains the CTI components that interface with applications. With CTI Manager, applications have access to resources and functionality of all Cisco CallManagers in the cluster and have improved failover capability. One or more CTI Managers can exist

on an individual server. An application (JTAPI/TAPI) can have simultaneous connections to multiple CTI Managers; however, an application can only use one connection at a time to open a device with media termination.

Cisco MOH Audio Translator

The Cisco MOH Audio Translator service converts audio source files into various codecs so that they can be used by the MOH feature. When you install the Cisco IP Voice Media Streaming Application service, Cisco CallManager automatically installs this service.

The Cisco MOH Audio Translator service automatically translates audio files that you place in the input directory. The installation program creates this input directory during installation in the following location: c:\Cisco\DropMOHAudioSourceFilesHere. If you want to change the input directory, modify the MOHSourceDirectory service parameter.

Once the Cisco MOH Audio Translator service translates the audio files, the Cisco MOH Audio Translator service places the source audio file and the translated file in the output directory on the default MOH TFTP server established during the Cisco MOH Audio Translator service installation. To change the output directory, modify the DefaultTFTPMOHFilePath parameter; however, make sure the path points to the default MOH TFTP server. The DefaultTFTPMOHFilePath parameter contains a universal naming convention (UNC) share name that displays in the format *computer name**directory name*.

Caution Cisco recommends that you install the Cisco MOH Audio Translator service on a different server than the one used for the Cisco CallManager server. The service can cause performance degradation and errors when translating audio files if it is installed on the Cisco CallManager server.

When the user assigns or maps the audio source file to an audio source number, the default MOH TFTP server copies the files into one directory, making them available for the MOH servers. The MOH servers download the audio files in the C:\Program Files\Cisco\MOH directory. For more detailed information on how the MOH feature accesses the files once the Cisco MOH Audio Translator service places them in the output directory, see the "Music On Hold" section on page 19-1.

Cisco RIS Data Collector

The Real-time Information Server (RIS) maintains real-time Cisco CallManager information and provides an interface through which the Cisco RIS Data Collector service and the SNMP Agent retrieve that information. One RIS exists on each node containing the Cisco CallManager service. The Cisco RIS Data Collector service provides an interface for applications, such as Cisco CallManager Serviceability and the Cisco CallManager Administration, to retrieve information stored in all RIS nodes in the cluster.

Service Installation and Configuration

You can install services from the Cisco CallManager CD or using the Cisco Service Configuration utility. To install services from the CD, check the check boxes next to the services you want to install from the CallManager Components window. To install services from the Cisco Service Configuration utility, choose **Start > Programs >Cisco CallManager 3.1 > Cisco Service Configuration**. When the utility opens, check the check boxes next to the services you want to install, and click **Apply**. Follow the online instructions to complete the installation. If a service is currently activated and you uncheck it and click **Apply**, Cisco CallManager shuts it down, removes it from the service registration table, and makes it unavailable for use.

Caution Do not deactivate the Cisco CallManager service using the Cisco Service Configuration utility. If it is inadvertently deactivated, contact the Cisco Technical Assistance Center (TAC).

After you install a service, you may need to start it. If you need to start a service, refer to the "Starting and Stopping Services" section in the *Cisco CallManager Administration Guide*.

Trace Settings

Cisco CallManager Serviceability provides a web-based trace tool to assist you and support personnel in troubleshooting Cisco CallManager problems. You configure trace parameters for Cisco CallManager services that are available on any Cisco CallManager server in the cluster. For more information on configuring and using the trace tool, refer to the *Cisco CallManager Serviceability Administration Guide*.

Services Configuration Checklist

Table 10-2 lists the steps for installing and configuring services.

Table 10-2 Services Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Install the services you want from the Cisco CallManager CD or from the Cisco Service utility.	*Installing Cisco CallManager Release 3.1*
Step 2	Configure the appropriate service parameters.	Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 3	Start the service.	Starting and Stopping Services, *Cisco CallManager Administration Guide*
Step 4	Troubleshoot problems using the Cisco CallManager Serviceability trace tool, if needed.	*Cisco CallManager Serviceability Administration Guide*

Where to Find More Information

Related Topics

- Conference Bridges, page 17-1
- Music On Hold, page 19-1

- Media Termination Points, page 20-1
- Cisco TFTP, page 8-1
- Understanding Cisco WebAttendant, page 30-1
- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- Starting and Stopping Services, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Installing Cisco CallManager 3.1*
- *Cisco CallManager Serviceability Administration Guide*

CHAPTER 11

Auto-Registration

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

Understanding Auto-Registration

Use auto-registration if you want Cisco CallManager to assign directory numbers automatically to new phones when you plug these phones into your network.

Caution Cisco CallManager disables auto-registration by default. Enabling auto-registration carries a security risk in that "rogue" phones can automatically register with Cisco CallManager. You should enable auto-registration only for brief periods when you want to perform bulk phone adds.

Cisco CallManager disables auto-registration by default to prevent unauthorized connections to your network.

When you enable auto-registration, you specify a range of directory numbers that Cisco CallManager can assign to new phones as they connect to your network. As new phones connect to the network, Cisco CallManager assigns the next available directory number in the specified range. Once a directory number is assigned to

an auto-registered phone, you can move the phone to a new location, and its directory number remains the same. If all of the auto-registration directory numbers are consumed, no additional phones can auto-register with Cisco CallManager.

New phones auto-register with the primary Cisco CallManager in the Cisco CallManager group that has the Auto-Registration Cisco CallManager Group setting enabled. That Cisco CallManager automatically assigns each auto-registered phone to a default device pool based on the device type (see the "Device Defaults" section on page 4-9). After a phone auto-registers, you can update its configuration and assign it to a different device pool and a different Cisco CallManager (see the "Device Pools" section on page 4-7).

Auto-Registration Configuration Checklist

Table 11-1 lists general steps and guidelines for using auto-registration.

Table 11-1 Auto-Registration Configuration Checklist

Configuration Steps		Procedures and related topics
Step 1	Configure only one Cisco CallManager in the cluster to use for auto-registration. Always enable or disable auto-registration on this Cisco CallManager only. If you want to shift the auto-registration function to another Cisco CallManager in the cluster, you must reconfigure the appropriate Cisco CallManagers, the Default Cisco CallManager Group, and possibly the default device pools.	Refer to the "Cisco CallManager Configuration"section in the *Cisco CallManager Administration Guide*.
Step 2	Configure the Default Cisco CallManager Group as the auto-registration group. Choose the auto-registration Cisco CallManager from Step 1 as the primary Cisco CallManager in this group.	See the "Cisco CallManager Groups" section on page 4-1. Refer to the "Cisco CallManager Group Configuration"section in the *Cisco CallManager Administration Guide*.

Table 11-1 Auto-Registration Configuration Checklist (continued)

Configuration Steps		Procedures and related topics
Step 3	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.	See the "Partitions and Calling Search Spaces" section on page 12-1. Refer to the "Calling Search Space Configuration" section in the *Cisco CallManager Administration Guide*.
Step 4	Configure the Default device pool for auto-registration by assigning the Default Cisco CallManager Group and auto-registration calling search space to it. If you are configuring a separate default device pool for each device type, assign the Default Cisco CallManager Group and auto-registration calling search space to each of the default device pools.	See the "System-Level Configuration Settings" section on page 4-1. Refer to the "Device Pool Configuration"and "Device Defaults Configuration" sections in the *Cisco CallManager Administration Guide*.
Step 5	Enable auto-registration only during brief periods when you want to install and auto-register 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 CallManager.	Refer to the "Enabling Auto-Registration" and "Disabling Auto-Registration" sections in the *Cisco CallManager Administration Guide*.
Step 6	Install the devices that you want to auto-register.	Refer to the installation instructions that come with your IP phones and gateways.
Step 7	Reconfigure the auto-registered devices and assign them to their permanent device pools.	Refer to the *Bulk Administration Tool Administration Guide* or the "Cisco IP Phone Configuration" and "Gateway Configuration" sections in the *Cisco CallManager Administration Guide*.

Where to Find More Information

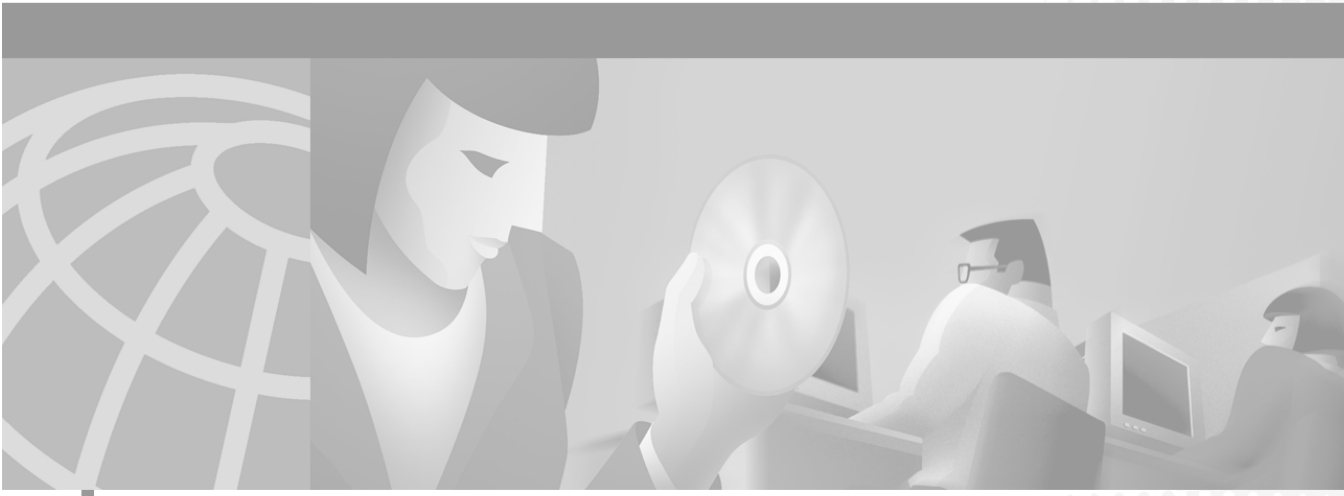
Related Topics

- System-Level Configuration Settings, page 4-1
- Redundancy, page 6-1
- Cisco CallManager Configuration, *Cisco CallManager Administration Guide*
- Cisco CallManager Group Configuration, *Cisco CallManager Administration Guide*
- Device Pool Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Bulk Administration Tool Administration Guide*

Cisco Systems



PART 3

Dial Plan Architecture

CHAPTER 12

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 CallManager.

This section covers the following topics:

Understanding Partitions and Calling Search Spaces

A partition comprises a logical grouping of directory numbers (DNs) and route patterns with similar reachability characteristics. Devices typically placed in partitions include DNs and route patterns. These are entities associated with DNs that users dial. For simplicity, partition names usually reflect their characteristics, such as "NYLongDistancePT," "NY911PT," and so on. When a DN or route pattern is placed into a certain partition, this creates a rule that specifies what devices can call that device or route list.

A calling search space comprises an ordered list of partitions that users can look at before being allowed to place a call. Calling search spaces determine which partitions calling devices, including IP phones, soft phones, 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 receives 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 the Cisco CallManager can respond.

Partitions do not significantly impact the performance of digit analysis, but every partition specified in a calling device's 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 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.

Examples

Calling search spaces determine which partitions calling devices search when attempting to complete a call.

For example, assume a calling search space named “Executive” has four partitions: NYLongDistance, NYInternational, NYLocalCall, and NY911. Assume another calling search space named “Guest,” includes two partitions: “NY911” and NYLocalCall.

If the Cisco IP phone associated with a phone or line is in the “Executive” calling search space, the search looks at partitions “NYInternationalCall,” “NYLongDistance,” “NYLocalCall,” and “NY911” when attempting to initiate the call. Users calling from this number can place international calls, long-distance calls, local calls, and calls to 911.

If the Cisco IP phone associated with a phone or line is in the "Guest" Calling Search Space, the search looks only at the "NYLocalCall" and "NY911" partitions when initiating the call. If a user 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 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.

Where to Find More Information

Related Topics

- Understanding Route Plans, page 13-1

Additional Cisco Documentation

- Partition Configuration, *Cisco CallManager Administration Guide*
- Calling Search Space Configuration, *Cisco CallManager Administration Guide*

CHAPTER 13

Understanding Route Plans

The Route Plan drop-down list on the menu bar allows you to configure Cisco CallManager route plans using route patterns, route filters, route lists, and route groups.

This section contains descriptions of the following route plan concepts:

Route Plan Overview

The Cisco CallManager uses the route plan to route both internal calls and external, public switched telephone network (PSTN) calls.

Route patterns, route filters, route lists, and route groups 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, or to a route list that contains one or more route groups. Route groups determine the order of preference for gateway and port 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 from being routed that are otherwise allowed by a route pattern. 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. It includes any number that can be dialed and is recognized in North America.

Route patterns represent all valid digit strings. When you assign a directory number to a Cisco IP phone, you assign it a route pattern (the directory number is the route pattern). Cisco Analog Access Trunk Gateways, Cisco Digital Access Trunk Gateways, Cisco MGCP gateways, H.323-compliant gateways also use route patterns. Cisco gateways can route ranges of numbers with complex restrictions and manipulate directory numbers before the Cisco CallManager passes them on to an adjacent system. The adjacent system can be a central office (CO), a private branch exchange (PBX), or a gateway on another Cisco CallManager system.

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, in Figure 13-1 shows Cisco Digital Access Gateway 1 designated as the first choice for routing outgoing calls to the PSTN.

Tips 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.

Note A gateway port can only belong to one route group; however, a route group can be assigned to multiple route lists.

Figure 13-1 shows the effects of using route patterns with Cisco Digital Access 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.

Note If a route pattern is associated with a gateway, then if all the resources of that gateway are used, the call is not routed.

Figure 13-1 Route Plan Summary Diagram for Cisco Digital Access Gateways

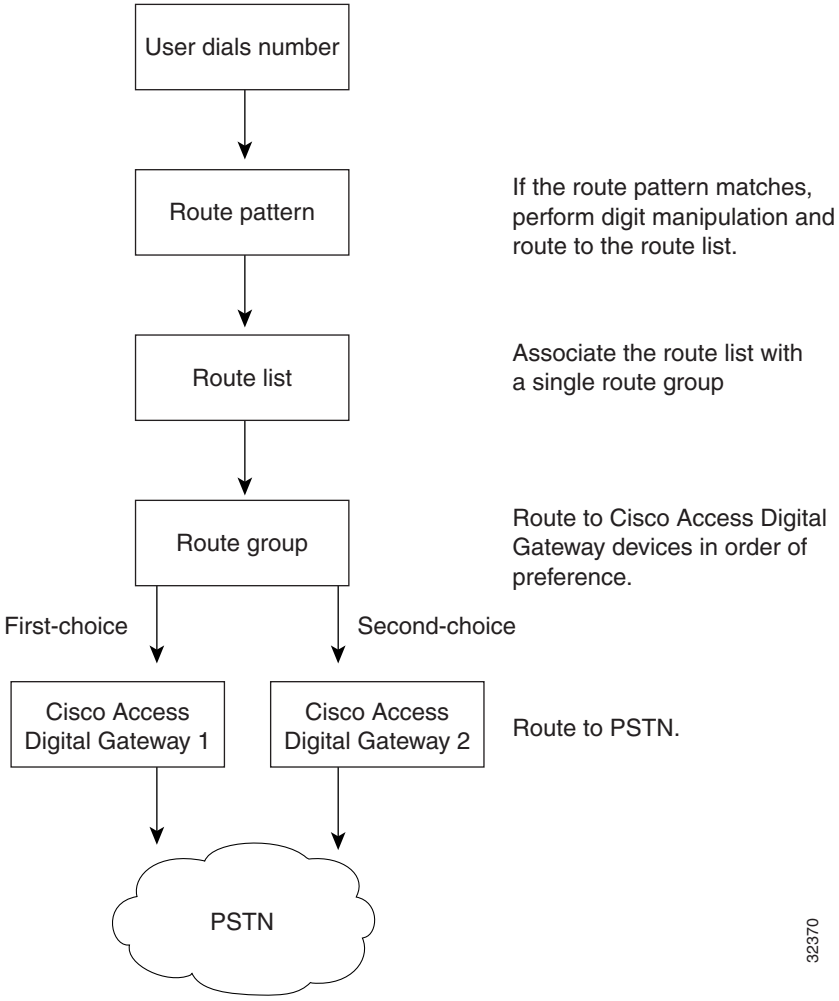
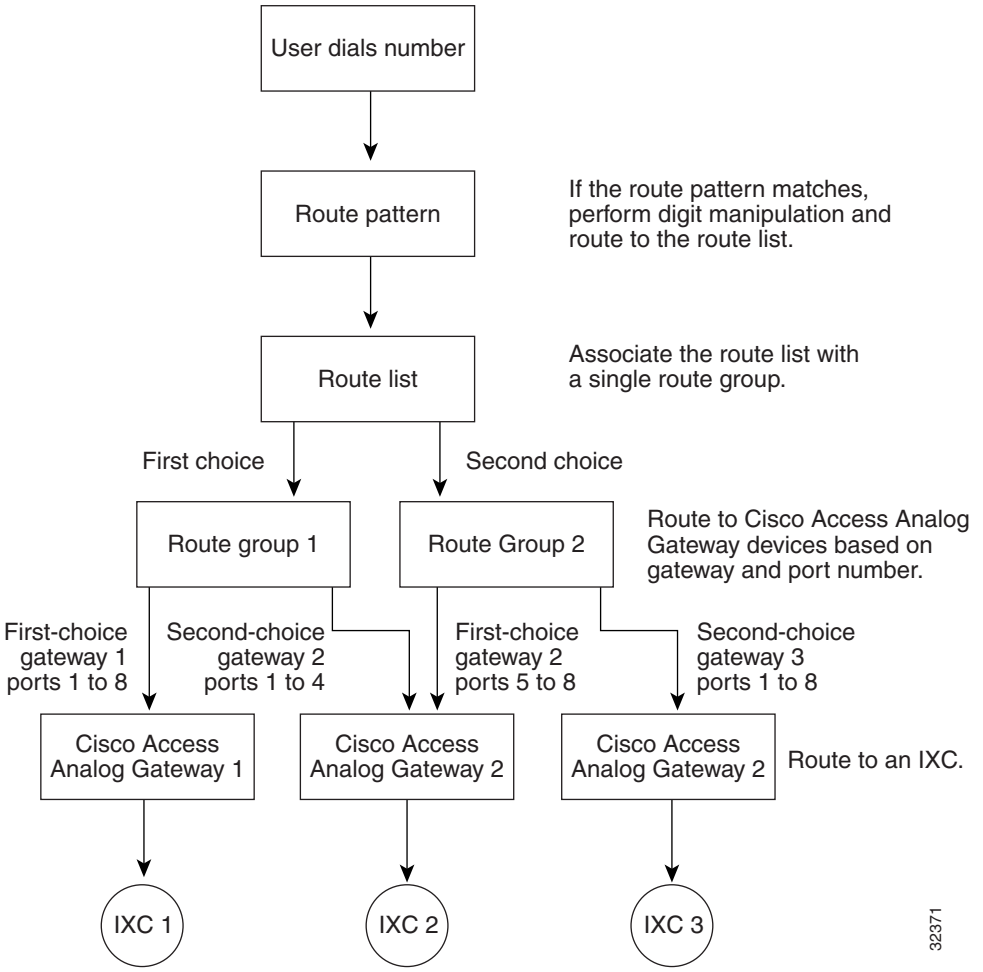


Figure 13-2 shows the effects of using route patterns with Cisco Analog Access Gateways. This example assigns the route pattern to a route list, and that route list associates with two route groups. Route group 1 associates with ports 1 through 8 on gateway 1, which routes all calls to interexchange 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 selected based on 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 13-2 Route Plan Summary Diagram for Cisco Analog Access Gateways



Route Pattern Wildcards and Special Characters

Route pattern wildcards and special characters allow a single route pattern to match a range of numbers (addresses). Also use these wildcards and special characters to build instructions that enable the Cisco CallManager to manipulate a number before sending it to an adjacent system.

The "Special Characters and Settings" section on page 20-1 describes the wildcards and special characters supported by Cisco CallManager.

Closest-Match Routing

Closest-match routing process routes a call using the route pattern that most closely matches the dialed number. When the Cisco 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 using that route pattern.

When two configured route patterns match exactly the same number of addresses in different partitions, Cisco CallManager chooses the route pattern based on order in which the partitions are listed in the calling search space. (Cisco CallManager chooses the route pattern from the partition that appears first in the calling search space.)

If two configured route patterns match exactly the same number of addresses in a partition, the Cisco CallManager arbitrarily chooses one. The following paragraphs explain why such exact matches signify an unusual occurrence.

It is possible to configure several route patterns that 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. Since 89XX matches a narrower range of addresses than 8XXX, the Cisco CallManager delivers the call to the device assigned the routing pattern 89XX.

Using the @ wildcard character in a route pattern requires additional consideration.

The number 92578912 matches both of the following route patterns: 9.@ and 9.XXXXXXX. Even though both of 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]XXXXXX. Since the number 2578912 more closely matches [2-9]XXXXXX than it does XXXXXXX, the 9.@ route pattern provides the closest match for routing.

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 that access code is not expected by the PSTN switch.

The "Special Characters and Settings" section on page 20-1 lists DDIs and describes the effects of applying each DDI to a dialed number.

Route Patterns

Cisco CallManager uses route patterns to route or block both internal and external calls. A directory number specifies a type of specific route pattern that is applied to a Cisco IP Phone. Gateways and Cisco IP phones can also use more complex route patterns that can contain wildcards.

Caution If a gateway has no route pattern associated with it, or it does not belong to a route group, it cannot route/block any calls.

Tips You must reset gateways for new or updated routing information to be recognized. Resetting the gateway may result in a dropped call.

The simplest route pattern just specifies a set of one or more digits. For example, the number 8912 specifies a route pattern. When assigned to a Cisco Access gateway or a route list, the Cisco CallManager directs any calls to 8912 to the assigned device.

Considerations for Using Route Patterns

When using route patterns, take the following considerations into account:

- If the route pattern contains an at symbol (@), the Discard Digits field can specify any of the PreAt discard digits instructions (DDIs).
- 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 don't use @, you must include the # in the routing pattern to be able to use the # character to signal the end of dialing.

Note The only Discard Digits instructions you may use with non-@ patterns are <None>, NoDigits, and PreDot.

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 using information provided by the administrator through a series of prompts.

The route plan generated by the external route plan wizard 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 used when you generate route plans with the external route plan wizard:

- Generated Route Filters, page 13-10
- Generated Route Groups, page 13-11

- Generated Route Lists, page 13-12
- Generated Route Patterns, page 13-14

Generated Route Filters

A generated route filter permits or restricts access through a route list using route patterns. The external route plan wizard associates each route list with a particular route filter. It names route filters using the TenantLocationCalltype convention, and appends the suffix RF to each route filter for easy identification.

Table 13-1 shows the seven types of route lists that use route filters. The examples shown in this table use specific route filter names and actual access and area codes for better readability.

Table 13-1 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 (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 (AREA-CODE DOES_NOT_EXIST) AND (LOCAL-AREA-CODE DOES_NOT_EXIST)
Toll bypass calls	Name: CiscoTollByPassToDallasRF Content: 9.@ where (AREA-CODE == 972) OR (AREA-CODE == 214)

Table 13-1 Route Lists and Associated Route Filters (continued)

Route List Type	Route Filter Name and Content Examples
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 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 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 imposed ensures that route groups associated with the local gateways are listed before the route groups associated with remote gateways. If needed, manually change the order after the route plan is generated.

Note Cisco CallManager treats all gateways belonging 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 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 available. Therefore, the total number of route lists depends on the local dialing scheme and the number of locations served by the route plan.

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 13-2 shows the eight types of route lists. The example shown in this table use specific route list names for better readability.

Table 13-2 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 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.

Table 13-2 Route List Types (continued)

Route List Type	Example Route List Name and Usage
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 using 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 using 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 using 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 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 has the prefix construction 9.@. The typical route pattern for routing a call to the PBX has 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, digit discard 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 served by that PBX. For example, if the access code used to direct calls to the adjacent PBX is 9 and the range of directory numbers served by that PBX is 1000 through 1999, then 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 call park numbers, call pickup numbers, conference numbers (Meet-Me numbers), route patterns, and translation patterns 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 pages, by selecting a route pattern, partition, route group, route list, call park number, call pickup number, conference number (Meet-Me number), or gateway.

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 Tools (BAT). The .csv file contains more detailed information than the web pages, including directory numbers (DN) for phones, route patterns, and translation patterns. Refer to "Route Plan Report" in the *Cisco CallManager Administration Guide* for more information.

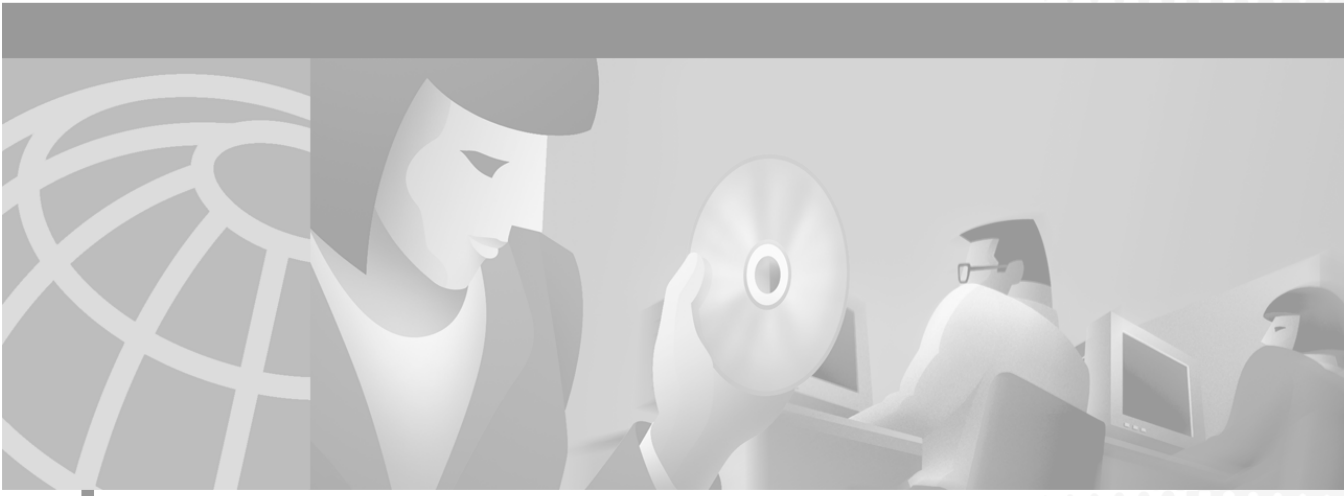
Where to Find More Information

Related Topics

- Partitions and Calling Search Spaces, page 12-1

Related Cisco Documentation

- Partition Configuration, *Cisco CallManager Administration Guide*
- Calling Search Space Configuration, *Cisco CallManager Administration Guide*
- *Cisco IP Telephony Network Design Guide*



PART 4

LDAP Directory and User Configuration

CHAPTER 14

Understanding the LDAP Directory

This chapter provides background information and deployment guidelines for integrating Cisco CallManager with an existing Lightweight Directory Access Protocol (LDAP) directory. This chapter is written for the administrator of the enterprise LDAP directory.

This chapter includes the following topics:

Cisco CallManager Directory

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

When you install the User Preferences plug-in, a number of configuration screens are added to the Cisco CallManager Administrator, which allows you to assign system resources for use by specific users. However, you need to use the native LDAP administration utilities to add user to the directory.

When you install the User Preferences plug-in, you are prompted to integrate the directory with one of the following enterprise LDAP directories:

- Microsoft Active Directory (AD)
- Netscape Directory Server

After the LDAP directory configuration is complete, you can upload completed workflow application files to the directory. The application server downloads the files to run workflow applications when you use the administration client to start a specific application. This design allows you to start workflow applications from anywhere in the network and run the applications on application servers throughout the enterprise network. Workflow applications communicate with the Cisco CallManager through JTAPI. It is also possible to run workflow applications on the same computer as the Cisco CallManager.

Using an Existing Enterprise Directory

If you integrate a directory with an existing LDAP directory, your directory schema will be extended to add new object classes for storing configuration information and workflow application logic. These extensions can be restricted to a specific branch of the LDAP directory and so should not affect the operation of the overall directory.

The Cisco CallManager Directory Services makes use of an LDAP auxiliary class to associate additional user properties (such as the mapping between the user name and a telephone extension) with the existing user object in your LDAP directory schema.

To use an existing directory, you must know the DN (distinguished name) and password for a user with administrator access to the branch of the directory where you wish to install Cisco CallManager. You will be prompted for this information during installation of the Cisco Customer Directory Configuration plug-in, if you choose to use an existing directory server.

You can use an LDIF (LDAP Interchange Format) file to add multiple entries to your LDAP directory in batch mode, or to add the attributes to an existing LDAP directory that are required to implement Cisco CallManager. The following example shows an LDIF file for adding a new user who will use Cisco CallManager.

Example 14-1 Sample LDIF File

```
dn: cn=jsmith-CCNProfile, ou=CCN, o=cisco.com
changeType: add
cn: jsmith-CCNProfile
objectclass: top
objectclass: ciscoCCNocAppProfile
ciscoatProfileOwner: John Smith
ciscoCCNatAllDevices: false
ciscoCCNatControlDevices: SEP0010EB001801
ciscoCCNatControlDevices: SEP0010EB001B01
ciscoCCNatControlDevices: SEP0010EB003CF0
ciscoCCNatControlDevices: SEP0010EB003EA3
ciscoCCNatControlDevices: SEP0010EB003EC4

dn: cn=jsmith-profile, ou=CCN, o=cisco.com
changeType: add
cn: jsmith-profile
objectclass: top
objectclass: ciscoocUserProfile
ciscoatProfileOwner: John Smith
ciscoatAppProfile: cn=jsmith-CCNProfile, ou=CCN, o=cisco.com

dn: cn=John Smith, ou=CCN, o=cisco.com
changeType: add
cn: John Smith
givenName: John
sn: Smith
mail: jsmith
userPassword: jsmith
objectclass: top
objectclass: inetOrgPerson
objectclass: ciscoocUser
ciscoatUserProfile: cn=jsmith-profile, ou=CCN, o=cisco.com
```

Extending the Enterprise Directory Schema

You need an LDAP administrator DN (distinguished name) and password to install Cisco CallManager on a production server. This DN should have read/write/modify privileges for the specific branch of the directory where the Cisco CallManager configuration information will be stored. In addition, the installation program will need to extend the user object in the enterprise directory schema to support additional Cisco IP Telephony network-specific attributes.

After the installation of Cisco CallManager on the production server, the enterprise directory is extended to add a new branch for Cisco CallManager configuration information.

Because all configuration information for users and applications is contained in a single branch of the enterprise directory, Cisco CallManager only requires read access to other branches of the enterprise directory.

On the other hand, only Cisco CallManager requires add or modify privileges to the Cisco IP Telephony network branch of the enterprise directory. It should be emphasized to the enterprise directory administrator that the information in this branch should only be modified using the Cisco CallManager Administrator or the Application Administration pages. If modifications are made with native LDAP tools, the configuration required to run Cisco CallManager can become corrupted and Cisco CallManager may have to be reinstalled.

Migrating to an Enterprise Directory

The Cisco CallManager administrator coordinates with the enterprise directory administrator to migrate the configuration information to the enterprise directory and to integrate Cisco CallManager with the user entries in the enterprise directory. The LDIF file can be modified to only add the auxiliary class attributes to the existing user objects, after the enterprise directory is extended by the Cisco CallManager installation.

Managing User Entries in an Enterprise Directory

After installing Cisco CallManager on the production server, users are added to the enterprise directory by the enterprise directory administrator. The enterprise directory administrator may use an LDIF file for bulk insert of configuration information for the existing users to enable them to use Cisco CallManager. Occasionally, when a few users are added to the enterprise directory, the Cisco CallManager administrator may use the Cisco CallManager Administrator User pages to configure the new users.

Enterprise Directory Replication

When implementing the Cisco CallManager system, you must consider the way the directory is replicated and partitioned to ensure adequate performance of Cisco CallManager and the other components of the system. The Cisco CallManager workflow framework has been designed to work with enterprise LDAP directories, and the way that partitions of these directories are distributed and replicated will directly affect system performance.

With this kind of geographic distribution, it is essential that the directory servers in each region are partitioned and replicated correctly so that Cisco CallManager has local access to the directory information it needs.

Where to Find More Information

Related Topics

- Cisco CallManager Groups, page 4-1
- Date/Time Groups, page 4-2
- Regions, page 4-3
- Device Pools, page 4-7
- Device Defaults, page 4-9
- Enterprise Parameters, page 4-9
- Call Admission Control, page 4-10

- System Configuration Checklist, page 4-11
- Cisco TFTP, page 8-1

Additional Cisco Documentation

- Enterprise Parameters Configuration, *Cisco CallManager Administration Guide*
- Device Support, *Cisco CallManager Administration Guide*
- Cisco JTAPI Installation and Configuration, *Cisco CallManager Administration Guide*
- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- Starting and Stopping Services, *Cisco CallManager Administration Guide*
- *Installing Cisco CallManager 3.1*
- *Cisco CallManager Serviceability Administration Guide*

CHAPTER 15

Managing User Directory Information

The User option in the Cisco CallManager Administration allows the administrator to add, search, display, and maintain information about Cisco CallManager users. This chapter describes the options for managing user directory information.

Refer to Adding a New User section of the *Cisco CallManager Administration Guide* for more procedures on adding users and configuring application profiles.

Refer to the Searching the Global Directory section of the *Cisco CallManager Administration Guide* for procedures on searching for users and updating information on existing users.

This chapter includes the following topics:

How Cisco JTAPI Uses the Directory

Cisco JTAPI uses the directory to determine which devices it can control and provides an interface method for getting the MAC address of the calling party, such as a user initiating the Extension Mobility Login.

After you install Cisco JTAPI, you have access to the Cisco 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.

Searching the Global Directory

The Global Directory for Cisco CallManager contains every user within a Cisco CallManager directory. Cisco CallManager uses Lightweight Directory Access Protocol (LDAP) to interface with a directory that contains user information.

You can access the Global Directory by using either a basic or an advanced user search.

Refer to the Searching the Global Directory section of the *Cisco CallManager Administration Guide* for procedures on searching for users and updating information on existing users.

For a description on adding a new user, see "Adding a User" section on page 15-4.

Related Topics:

- Using Basic Search, page 15-3
- Using Advanced Search, page 15-3

Using Basic Search

The Basic User search utility searches the first name, last name, and user ID fields for matches of any substring that you enter as search criteria. For example, if you enter “li” in the search field, the search results would include users whose first name, last name, or user ID match that substring, as indicated in the following list:

Last Name	First Name	User ID
Johnson	Charlie	cjohnson
Ni	Liang	lni
Collins	Manny	mcollins
Lin	Mike	michaell
Ivey	Gabriel	Gabrieli

If you enter two or more substrings separated by spaces, the search will look for matches of any of the substrings in any of the three search fields.

The following procedure contains information about how to use the Global Directory Basic User Search engine.

Using Advanced Search

The Advanced User Search utility has a built-in Boolean logic to perform more complex searches. You can enter search criteria using the following fields:

- First Name
- Last Name
- User ID
- Department Number

If you enter two or more names or substrings separated by spaces in any one field, the search will interpret the request with the OR relationship operator and will look for matches where any of your specified criteria is true. For example, if you enter “john jerry”, the search will return all users whose first names are John or Jerry.

If you enter a substring in two or more search fields, the search will interpret the request with the AND relationship operator and look for matches where all criteria is true. For example, if you enter “Ling” for first name and “Chu” for last name, the search will return the user named Ling Chu.

Tips Use ORs with multiple entries in a single field and ANDs across fields. For example, if you enter

First Name: john jane
Last Name: jones smith
UserID: jjones jsmith

the search will be for (firstname=”john” OR “jane”) AND lastname=”jones” OR “smith”) AND (userid=”jjones” OR “jsmith”).

Adding a User

Generally, completing user information is optional; the devices function whether or not you complete this information. However, information that you enter here is also accessed by Directory Services, Cisco WebAttendant, and the Cisco IP Phone User Options panes. If you want to provide these features to your users, you must complete the information in the User Information pane for all users and their directory numbers, and also for resources such as conference rooms or other areas with phones (this is useful for Cisco WebAttendant).

Refer to the chapter on Adding a New User in the *Cisco CallManager Administration Guide* for more procedures on adding users and configuring application profiles

Application Profiles

After you add a new user, options in the Application Profile section of the User Information pane in the Cisco CallManager Administration allows you to configure the user profile. These profiles allows each user to personalize phone features, mobility, and Cisco IP SoftPhone capability.

For information on configuring Application Profiles for users, refer to the "Configuring Application Profiles" section of the *Cisco CallManager Administration Guide*.

Device Association

Associating devices to a user gives the user control over specified devices. Users 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.

The User Device Assignment window comprises a device filter section and a list of available devices.

Available Device List Filters

The device filter allows you to limit your list of devices by entering search criteria based on all or part of the device name, description, or directory number. To limit the list of available devices to a specific selection, enter the criteria by which you want to search using the following methods:

- Choose device name, description, or directory number.
- Choose the comparison operator.
- Enter a text or number entry.

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.

Available Devices

Once you have specified the search criteria to display devices, all matching available devices appear in the Available Devices list. The list displays in groups of 20 devices and can be navigated using the buttons at the bottom of the window.

You can page through the device list by clicking **First**, **Previous**, **Next**, and **Last**, or you can jump to a specific pane by entering the page number in the pane entry box and then clicking **Page**.

If you are modifying the device assignment for an existing user, the devices previously assigned to that user appear in a group at the beginning of the device list.

You can associate one or more devices to the user by checking the checkbox next to that device. If a device has multiple extensions associated with it, each line extension appears in the list. You need to choose only one line extension to choose all the lines associated with that device.

To assign devices to a user, you must access the User Information window for that user. Refer to the "Searching the Global Directory" section on page 15-2 for information on accessing information on existing users.

Auto Attendant

The Automated Attendant (AA) service answers incoming calls and prompts the caller for a user name or extension. The directory is scanned for a match to resolve the user name or extension and transfers the caller to the appropriate endpoint.

The AA service requires a unique telephone keypad numerical representation of each user name. The mapping generates after you add a new user. The representation is an alphabetical mapping of the last name, first name, and the middle initial (LastFirstM) to corresponding keys on the telephone. Subsequently, the number is checked against the number representations of all the existing users in the user table.

If the number is unique, it is then used to find the least number of digits required to identify a user. Otherwise, if a same name or same numerical mapping occurs, a prompt returns indicating a duplicate key. At this point, you can either change the user's name (through nicknames or removal of middle initials) or allow duplicates.

Extension Mobility

Extension Mobility allows a user to configure a Cisco IP Phone 7940 or Cisco IP Phone 7960 to appear as that user phone temporarily. 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.

The center of the login processing is the Workflow Engine. User and device information is sent via DTMF and JTAPI to the Workflow Engine, which makes the information available within the Workflow.

User Device Profiles are used to support the Extension Mobility feature. The User Device Profile includes the following information:

- Name
- Description
- Phone template
- Add-on modules
- Directory numbers
- Device-subscribed services
- Speed Dial information

An authentication scheme authenticates the user. The Workflow 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 based on the MAC address of the device on which the user wants their profile to reside

The result of the request returns a dialog prompt on the device of the calling user.

The logout process is also the Workflow Engine. The device name is sent to the workflow engine using JTAPI. The workflow engine sends a logout request to t he login service, and the user receives a dialog prompt on the device.

SoftPhone

You can associate a device (line) to a user as a Cisco IP SoftPhone. This will enable the user to use their desktop PC to place and receive telephone calls and to control an IP telephone.

Include the IP Address or host name in the Associated PC field.

For more information, refer to the *Cisco IP SoftPhone Administrator Guide*

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/softphon/

User Directory Guidelines and Tips

The following system requirements and limitations apply to conference bridges:

- Conference devices configured for software support G.711 codecs by default.
- The maximum limit for a software conference with IP voice media streamer is 48.
- The maximum limit for a software conference with voice media streamer on a separate non-Cisco CallManager Media Convergence Server (MCS) is 128.
- Conference devices configured for hardware provide transcoding for G.711, G.729, G.723, G711 GSM Full Rate (FR), and G711 GSM Enhanced Full Rate (EFR) codecs.
- The maximum number of full-duplex streams per MTP WS-X6608 port is 32.

Managing User Directory Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Search for user in the Global Directory.	Searching the Global Directory, *Cisco CallManager Administration Guide*
Step 2	Add user.	Adding a New User, *Cisco CallManager Administration Guide*
Step 3	Configure the Application Profiles	Adding a New User, *Cisco CallManager Administration Guide* Device Profile Configuration, *Cisco CallManager Administration Guide*
Step 4	Add a Conf button for Ad Hoc or MMConf button for the Meet-Me conference to the phone templates, if needed. You only need to do this for older Cisco IP Phone 12 SP, 12 SP+, and 30 VIP phones.	Modifying Phone Button Templates, *Cisco CallManager Administration Guide*
Step 5	Notify users of the features they have available for use.	The *Cisco IP Phone 7960/7940 Getting Started Guide* contains instructions on how users access various features on the Cisco IP phone.

Where to Find More Information

Related Topics

- Device Profile Configuration, *Cisco CallManager Administration Guide*
- Phone Button Template Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Cisco WebAttendant Configuration, *Cisco CallManager Administration Guide*
- Conference Bridge Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

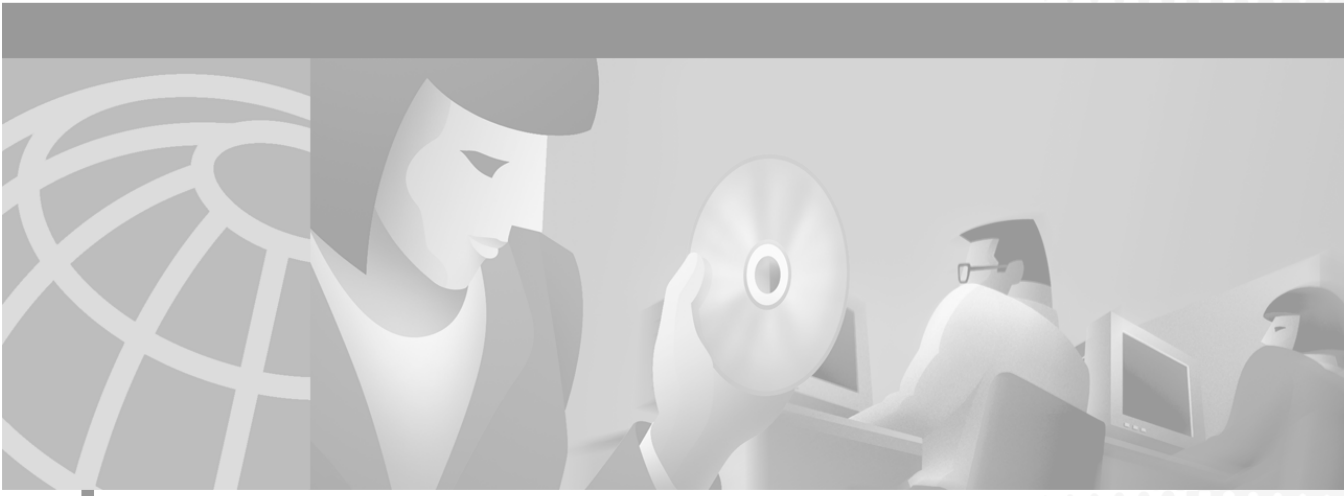
- *Cisco IP SoftPhone Administrator Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/softphon/
- *Cisco IP SoftPhone User Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/softphon/
- Cisco IP Phone user documentation and release notes (all models)

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

Cisco Systems



PART 5

Media Resources

CHAPTER 16

Media Resource Management

Cisco IP telephony functionality requires the use of media resources. Media resources provide services such as transcoding, conferencing, music on hold, and media termination. In previous releases, these resources were accessible only to the local Cisco CallManager with which the media resources registered but not available to all Cisco CallManagers within the cluster. The media resource manager allows all Cisco CallManagers within the cluster to share these media resources.

The media resource manager enhances Cisco CallManager features by making Cisco CallManager more readily able to deploy media termination point, transcoding, conferencing and music on hold services. Distribution throughout the cluster uses resources to their full potential, making them more efficient and more economical.

This chapter covers the following topics:

Understanding Media Resources

Media resource management provides access to media resources for all Cisco CallManagers in a cluster. Every Cisco CallManager contains a software component called a media resource manager. The media resource manager locates the media resource necessary to connect media streams to complete a feature. The Cisco CallManager interfaces to these media resources using Skinny protocol.

The media resource manager manages the following media resource types:

- Music On Hold (MOH) server
- Unicast conference bridge (CFB)
- Media streaming application server (software media termination point)
- Transcoder (XCODE)

The following reasons explain why resources are shared:

- To allow both hardware and software devices to coexist within a Cisco CallManager
- To enable Cisco CallManager to share and access resources available in the cluster
- To enable Cisco CallManager to do load distribution within a group of similar resources
- To enable Cisco CallManager to allocate resources based on user preferences

Initialization of the Cisco CallManager creates a media resource manager. Each media termination point, music on hold, transcoder, and conference bridge device 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 available in the system, also tracking the devices that have available resources.

When a media device registers, Cisco 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 CallManager no longer needs the resource, resource deallocation occurs. Cisco 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

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.

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 a-law to mu-law.

For each media termination point device defined in the database, Cisco CallManager creates a media termination point control process. This media termination point control process registers with the media resource manager when it initializes. The media resource manager keeps track of these media termination point resources and advertises their availability 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 CallManager.

For each unicast bridge device defined in the database, Cisco CallManager creates a unicast control process. This unicast control process registers with the media resource manager when it initializes. The media resource manager tracks unicast stream resources and advertises their availability 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 defined in the database, Cisco CallManager creates a music on hold control process. This music on hold control process registers with the media resource manager when it initializes. The media resource manager tracks music on hold resources and advertises their availability throughout the cluster. Music on hold supports both unicast and multicast audio sources.

Media Resource Groups

Cisco 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.

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) 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 CallManagers within a given cluster.

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 device name.
- If the requested resource is not found, search the next media resource group in the media resource group list. Return the device name 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 CallManager comprises the following media resources: MOH1, MTP1, XCODE1, XCODE2, XCODE3. For calls requiring a transcoder, this Cisco 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 among the available resources according to the priority order 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:

- Media resource group list, configured on the Media Resource Group List Configuration window, is assigned either to a device or to a device pool.
- Call processing uses media resource group list in the device level if the media resource group list is selected.

- Call processing uses media resource group list in the device pool only if no media resource group list is selected in the device level.

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 CallManager allocates the software conference resource first; the hardware conference is not 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

Cisco CallManagers are designated as CM1 and CM2.

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 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. Only media termination point, transcoder, and music resources are available to the device.

Media Resource Group and Media Resource Group List Configuration Checklist

Table 16-1 provides a checklist to configure media resource groups and media resource group lists.

Table 16-1 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 CallManager Administration Guide*
Step 2	Assign device to the media resource group. (Order is not significant.)	Media Resource Group Configuration, *Cisco CallManager Administration Guide*
Step 3	Create a media resource group list. (Order is significant.)	Media Resource Group List Configuration, *Cisco CallManager Administration Guide*

Table 16-1 Media Resource Group/Media Resource Group List Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 4	Assign a media resource group to a media resource group list.	Media Resource Group List Configuration, *Cisco CallManager Administration Guide*
Step 5	Assign a media resource group list to a device or device pool.	Device Defaults Configuration, *Cisco CallManager Administration Guide* Device Pool Configuration, *Cisco CallManager Administration Guide*

Requirements and System Limits

The following lists detail the limits that apply to the various media resources.

Media Termination Point Limits

For media termination points, the following limits apply:

- Up to 128 full-duplex streams are configurable.
- With 128 configured streams, 64 resources are available for media termination point application.

Software Conference Limits

For software conferences, the following limits apply:

- Up to 128 full-duplex streams are configurable.
- With 128 streams, a software conference media resource can handle 128 users in a single conference or
- With 128 streams, a software conference media resource can handle up to 42 conferencing resources with three users per conference

Transcoder Limits

For transcoders, 48 streams register and provide up to 24 transcoding resources.

Hardware Conference Limits

For hardware conference, 32 streams register, so the hardware conference media resource can handle 32 users in a single conference or up to 10 conferencing resources with three users per conference.

Music On Hold Server Limits

For music on hold media resources, the following limits apply:

- Up to 500 simplex streams are configurable.
- With 500 configured streams, up to 500 resources are available for music on hold application.

Chapter 19, "Music On Hold," covers further music on hold details.

Monitoring Media Resources

Counters in the Performance Monitor software supplied with Windows2000 monitor media resource usage. Cisco CallManager statistics include these counters. Counters track the following media resource devices:

- Hardware conference
- Media termination point
- Music on hold
- Software conference
- Transcoder

Monitoring Media Termination Point Resources

The following counters monitor media termination point resources:

- MediaTermPointsActive—The number of media termination points currently in use
- MediaTermPointsAvailable—The number of media termination points currently registered with the Cisco CallManager but not currently in use
- MediaTermPointsOutOfResources—The number of times a media termination point was requested for a call, but no resources were available

Monitoring Transcoder Resources

The following counters monitor transcoder resources:

- TranscoderActive—The number of transcoders currently in use
- TranscoderAvailable—The number of transcoders currently registered with the Cisco CallManager but not currently in use
- TranscoderOutOfResources—The number of times a transcoder was requested for a call, but no resources were available

Monitoring Software Conference Resources

The following counters monitor software conference resources:

- UnicastSoftwareConferencesAvailable—The number of conferences currently registered with the Cisco CallManager but not currently in use
- UnicastSoftwareConferenceActive—The number of conferences currently in use
- UnicastSoftwareConferenceCompleted—The number of times a conference was completed
- UnicastSoftwareOutOfResources—The number of times a conference was requested for a call, but no resources were available

Monitoring Hardware Conference Resources

The following counters monitor hardware conference resources:

- UnicastHardwareConferenceActive—The number of hardware conferences currently in use
- UnicastHardwareConferenceAvailable—The number of hardware conferences currently registered with the Cisco CallManager but not currently in use
- UnicastHardwareConferenceCompleted—The number of times a hardware conference was completed
- UnicastHardwareConferenceOutOfResources—The number of times a hardware conference was requested for a call, but no resources were available

Monitoring MOH Resources

The following PerfMon counters monitor MOH resources:

- MOHMulticastActiveStreams
- MOHMulticastAvailableStreams
- MOHOutOfResources
- MOHTotalMulticastStreams
- MOHTotalUnicastStreams
- MOHUnicastActiveStreams
- MOHUnicastAvailableStreams

Chapter 19, "Music On Hold," discusses MOH-related counters.

Where to Find More Information

Additional Cisco Documentation

- Media Resource Group Configuration, *Cisco CallManager Administration Guide*
- Media Resource Group List Configuration, *Cisco CallManager Administration Guide*
- Music On Hold Configuration, *Cisco CallManager Administration Guide*

CHAPTER 17

Conference Bridges

Conference Bridge for Cisco CallManager designates a software and hardware application designed to allow both Ad-Hoc and Meet-Me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Conference Bridge include the following features:

- Adding new participants to an existing conference call
- Ending a conference call
- Canceling a conference call
- Parking a conference call
- Transferring a conference call

Note The hardware model type for Conference Bridge contains a specific Media Access Control (MAC) address and device pool information.

This section covers the following topics:

Understanding Conference Devices

Cisco CallManager supports multiple conference devices to distribute the load of mixing audio between the conference devices. A component of Cisco CallManager called Media Resource Manager (MRM) locates and assigns resources throughout a cluster. The MRM resides on every Cisco CallManager and communicates with MRMs on other Cisco CallManagers.

Both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec they support. For software conference devices, you can adjust the number of streams. Hardware conference devices, however, support a fixed number of streams.

For conferencing, you must determine the total number of concurrent users (or audio streams) required at any given time. Then you create and configure a software conference device to support the calculated number of streams. One large conference, or several small conference, can use these audio streams.

Caution Although a single software conference device can be installed on the same PC as the Cisco CallManager, we strongly recommend against this. Installation of a conference device service on the same PC as the Cisco CallManager can adversely affect performance on the Cisco CallManager.

Note Conference devices that are configured for software support G.711 codecs by default. Conference devices configured for hardware provide transcoding for G.711, G.729, G.723, G711 GSM Full Rate (FR), and G711 GSM Enhanced Full Rate (EFR) codecs.

Hardware Conference Devices

Hardware-enabled conferencing provides the ability to support voice conferences in hardware. Digital Signaling 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 the Cisco CallManager.

MTP WS-X6608 DSP Service Card

The MTP WS-X6608 DSP service card provides DSP resources for both conference applications and transcoding applications. Hardware conference devices are fixed at 32 full-duplex streams per MTP WS-X6608 port; therefore, hardware conference devices support 32 divided by three (32/3), or 10, conferences. Users cannot change this value.

NM-HDV Network Modules

NM-HDV network modules (NM) provide DSP conferencing resources, which includes a maximum of 15 T1-549 DSPs in 5 SPMM slots or 3 DSPs per slot. The NM-HDV NM utilizes the VG200 platform.

NM-HDV-2E1-60 Module

NM-HDV-2E1-60 currently supports 30 channels of a high-complexity codec (such as G.729) and 60 channels of a medium-complexity codec (such as G.711). NM-HDV-2E1-60 supports a maximum of 90 channels of conferencing ports per module.

NM-HDV-2T1-48 Module

NM-HDV-2T1-48 supports 24 channels of high-complexity codecs and 48 channels of medium-complexity codecs. NM-HDV-2T1-48 supports a maximum of 72 channels of conferencing ports per module.

Note The minimum participant size for a conference is three.

Software Conferences Devices

Software conference devices support a variable number of audio streams. You can create and configure a software conference device and select 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 maximum number of audio streams is 128.

Using Different Types of Conferences: Meet-Me and Ad-Hoc

Cisco CallManager supports both Meet-Me conferences and Ad-Hoc conferences. Meet-Me conferences allow users to dial into a conference. Ad-Hoc conferences allow the conference controller to let only certain participants into the conference.

Meet-Me conferences require that a range of directory numbers be allocated for exclusive use of the conference. When a Meet-Me conference is set up, the conference controller selects 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 specified for that conference type has not been exceeded and when sufficient streams are available on the conference device.)

Initiating an Ad-Hoc Conference Bridge

The conference controller controls Ad-Hoc conferences. When you initiate an Ad-Hoc conference, Cisco CallManager considers you the conference controller. In an Ad-Hoc conference, only a conference controller can add participants to a conference. The conference controller can add any number of parties to the conference up to the maximum number of participants specified for Ad-Hoc conferences and provided that sufficient streams are available on the conference device.

When the conference controller initiates a conference call, the Cisco CallManager places the current call on hold, flashes the conference lamp, and provides dial tone to the user. At the dial tone, the conference controller dials the next conference participant and, when the user answers, presses Conference again to complete the conference. The Cisco CallManager then connects the conference controller, the first participant, and the new conference participant to a conference bridge. Each participant Cisco IP phone display reflects the connection to the conference.

Participants can leave a conference by simply hanging up. A conference continues even if the conference controller hangs up, although the remaining conference participants cannot add new participants to the conference.

Initiating a Meet-Me Conference Bridge

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 selects 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 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 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 CallManager ignores the signals.

The conference controller selects a directory number from the range specified for the conference device. The Cisco CallManager Administrator provides the Meet-Me conference directory number range to users so they can access the feature.

A conference continues even if you, the conference controller, hang up.

Conference Bridge Guidelines and Tips

The following system requirements and limitations apply to conference bridges:

- Conference devices configured for software support G.711 codecs by default.
- A software conference with IP voice media streamer cannot exceed the maximum limit of 48.
- A software conference with voice media streamer on a separate non-Cisco CallManager Media Convergence Server (MCS) cannot exceed the maximum limit of 128.

- Conference devices configured for hardware provide transcoding for G.711, G.729, G.723, G711 GSM Full Rate (FR), and G711 GSM Enhanced Full Rate (EFR) codecs.
- Full-duplex streams per MTP WS-X6608 port cannot exceed the maximum limit of 32.

Conference Bridge Configuration Checklist

Table 17-1 provides a checklist to configure conference bridge.

Table 17-1 Conference Bridge Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure the conference device(s).	Adding a Software Conference Device, *Cisco CallManager Administration Guide* Adding a Hardware Conference Device, *Cisco CallManager Administration Guide*
Step 2	Configure the Meet-Me Number/Pattern.	Adding a Meet-Me Number/Pattern, *Cisco CallManager Administration Guide*
Step 3	Add a Conf button for Ad Hoc or MMConf button for the Meet-Me conference to the phone templates, if needed. You only need to do this for older Cisco IP Phone 12 SP, 12 SP+, and 30 VIP phones.	Modifying Phone Button Templates, *Cisco CallManager Administration Guide*
Step 4	Notify users that the Conference Bridge feature is available.	The *Cisco IP Phone 7960/7940 Getting Started Guide* contains instructions on how users access conference bridge features on their Cisco IP Phone.

Updating Conference Bridge Configurations

For the changes to take effect, you must reset each Conference Bridge device after making updates. To do this, click **Update** and a message displays stating that the Conference Bridge device must be reset in order for the changes to take effect. Click **OK** and the pane refreshes showing the updated device information.

Where to Find More Information

Related Topics

- Server Configuration, *Cisco CallManager Administration Guide*
- Phone Button Template Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Partition Configuration, *Cisco CallManager Administration Guide*
- Conference Bridge Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Phone 7900 Family Administration Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/7900/
- Cisco IP Phone user documentation and release notes (all models)

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

CHAPTER 18

Transcoders

The Media Resource Manager (MRM) is responsible for resource registration and resource reservation of transcoders within a Cisco CallManager cluster. Cisco CallManager supports simultaneously 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

A transcoder takes the output stream of one codec and transcodes (converts) it from one compression type to another compression type. For example, it could take an output stream from a G.711 codec and transcode (convert) it in real time to a G.729 input stream. In addition, a transcoder provides MTP capabilities, and may be used to enable supplementary services for H.323 endpoints when required.

The Cisco CallManager invokes a transcoder on behalf of endpoint devices when the two devices are using different 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 in order to enable communications between them.

A transcoder requires specific hardware in order to run. The same hardware also supports Conference Bridges, transcoders, or PRI interfaces.

A transcoder provides a designated number of streaming mechanisms, each of which is capable of transcoding data streams between different codecs and enabling supplementary services, if required, for calls to H.323 endpoints.

Managing Transcoders with the Media Resource Manager

Transcoders are accessible by all Cisco CallManagers within a cluster through the Media Resource Manager (MRM). The MRM determines the number of transcoders needed for a call and allocates the appropriate number of connections.

The MRM makes use of Cisco 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 is created for each transcoder device defined in the database. Each transcoder registers with the MRM when it initializes. The MRM keeps track of the transcoder resources and advertises their availability throughout the cluster.

Transcoder Capacity

The maximum transcoding sessions per port is 24. The following lists the supported transcoding capacity and sessions per port:

- G711–G711 MTP: 24 (no DSP is involved)
- G729–G729 MTP: 24 (no DSP is involved)
- G711–G723 transcoding: 24

- G711–G729 transcoding: 24
- G711–GSM Full Rate (FR) transcoding: 24
- G711–GSM Enhanced Full Rate (EFR) transcoding: 24

For example, transcoder 1 is configured for 24transcoder resources. Transcoder 2 is also configured for 24 transcoder resources. If both transcoders register with the same Cisco CallManager, that Cisco CallManager maintains both sets of resources for a total of 48 registered transcoder resources.

The capacity of 24 transcoders is based on a packet size of 1 packet per 20 msec. The smaller packet size of 10 msec does not increase audio quality. Rather it reduces the total capacity of transcoder resources.

When the Cisco CallManager determines that the two endpoints of a call are using different codecs and cannot communicate directly, it inserts a transcoder into the call to transcode the datastreams between them. The transcoder is not visible to either the user or the endpoints involved in a call.

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 CallManager cluster. In this capacity, when the Cisco 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 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 is used to support MTP and transcoding functionality simultaneously.

If a transcoder resource is not available when it is needed, the call is connected without using a transcoder resource, and supplementary services are not available on that call.

Transcoder Failover and Failback

This section describes how transcoder devices failover and failback in the event that the Cisco CallManager to which they are registered becomes unreachable. Conditions that can affect calls associated with a transcoder device, such as transcoder 1reset or restart, are also explained.

Active Cisco CallManager becomes Inactive

The following describes the MTP device recovery methods when the MTP is registered to a Cisco CallManager that goes inactive.

- If the primary Cisco CallManager fails, the transcoder attempts to register with the next available Cisco CallManager in the Cisco CallManager Group specified for the device pool to which the transcoder belongs.
- The transcoder device re-registers with the primary Cisco CallManager as soon as it becomes available after a failure, and is currently not in use.
- An transcoder device is registered to a Cisco CallManager that becomes unreachable. The calls or conferences that were on that Cisco CallManager will register with the next Cisco CallManager in the list.
- If a transcoder attempts to register with a new Cisco CallManager and the register acknowledgment is never received, the transcoder registers with the next Cisco CallManager.

Resetting Registered Transcoder Devices

The transcoder devices will un-register and then disconnect after a hard or soft reset. After the reset completes, the devices re-register with the primary Cisco CallManager.

Transcoder Configuration Checklist

Table 18-1 provides a checklist to configure transcoder.

Table 18-1 Transcoder Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Determine the number of transcoder resources needed and the number of transcoder devices needed to provide these resources.	Transcoder Configuration, *Cisco CallManager Administration Guide*
Step 2	Verify that the Cisco IP Voice Media Streaming Application service is installed and running on the server to which you are adding a transcoder.	*Cisco CallManager Serviceability Administration Guide*
Step 3	Add and configure the transcoders.	Transcoder Configuration, *Cisco CallManager Administration Guide*
Step 4	Add the new transcoders to the appropriate Media Resource groups.	Chapter 16, "Media Resource Management" Media Resource Group Configuration Settings, *Cisco CallManager Administration Guide*
Step 5	Restart the Transcoder device.	

Where to Find More Information

Related Topics

- **Cisco IP Voice Media Streaming Application Service**
- Chapter 16, "Media Resource Management"
- Chapter 20, "Media Termination Points"
- Media Resource Group Configuration, *Cisco CallManager Administration Guide*
- Media Resource Group Configuration Settings, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Telephony Network Design Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network/

CHAPTER 19

Music On Hold

The integrated Music On Hold (MOH) feature allows users to place on-net and off-net users on hold with music streamed from a streaming source. The Music On Hold feature allows two types of hold:

- End-user hold
- Network hold, which includes transfer hold, conference hold, and call park hold

Music On Hold also supports other scenarios where recorded or live audio is needed.

This chapter covers the following topics:

Understanding Music On Hold

The following sections explain the Music On Hold feature by providing definitions, service characteristics, feature functionality with examples, and supported features.

Music On Hold Definitions

In the simplest instance, music on hold takes effect when phone A is talking to phone B, and phone A places phone B on hold. If Music On Hold (MOH) resource is available, phone B listens to music streamed from a music on hold server.

The following definitions provide important information for the discussion that follows:

- MOH server—A software application that provides music on hold audio sources and connects a music on hold audio source to a number of streams.
- Media resource group—A logical grouping of media servers. You may associate a media resource group with a geographical location or a site as desired. You can also form media resource groups to control server usage or desired service type (unicast or multicast).
- Media resource group list—A list that comprises prioritized media resource groups. An application can select required media resources among available ones according to the priority order defined in a media resource group list.
- Audio source ID—An ID that represents an audio source in the music on hold server. The audio source can be either a file on a disk or a fixed device from which a source stream obtains the streaming data. One cluster can support up to 51 audio source IDs (1 to 51). Each audio source (represented by an audio source ID) can stream as unicast and multicast mode, if needed.
- Holding party—In an active, two-party call, the party that initiates a hold action (either user hold or network hold). Example: if party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party A is the holding party.
- Held party—In an active, two-party call, the party that does not initiate a hold action, but is involved. Example: if party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party B is the held party.

The following audio source ID selection rules apply for selecting audio source IDs and media resource group lists:

- The system administrator, not the end user, defines (configures) audio source IDs.
- The system administrator chooses (configures) audio source IDs for device(s) or device pool(s).
- Holding parties define which audio source ID applies to held parties.
- Cisco CallManager implements four levels of prioritized audio source ID selection with level four as highest priority and level one as lowest priority.
  - The system selects audio source IDs at level four, which is directory/line-based, if defined. (Devices with no line definition, such as gateways, do not have this level.)
  - If no audio source ID is defined in level four, the system searches any selected audio source IDs in level three, which is device based.
  - If no level four nor level three audio source IDs are selected, the system selects audio source IDs defined in level two, which is DevicePool-based.
  - If all higher levels have no audio source IDs selected, the system searches level one for audio source IDs, which are service-wide parameters.

The following media resource group list selection rules apply:

- Held parties determine which media resource group list a Cisco CallManager uses to allocate a music on hold resource.
- Two levels of prioritized media resource group list selection exist:
  - Level two media resource group list provides the higher priority level, which is device based. Cisco CallManager uses the media resource group list at the device level if such a media resource group list is defined.
  - Level one media resource group list provides the lower priority level, which is an optional DevicePool parameter. Cisco CallManager uses the DevicePool level media resource group list only if no media resource group list is defined in the device level for that device.
- If no media resource group lists are defined, Cisco CallManager uses the system default resources. System default resources comprise resources that are not assigned to any existing media resource group. System default resources are always unicast.

Music On Hold Characteristics

The integrated Music On Hold feature allows users to place on-net and off-net users on hold with music streamed from a streaming source. This source makes music available to any possible on-net or off-net device placed on hold. On-net devices include station devices and applications placed on hold, consult hold, or park hold by an interactive voice response (IVR) or call distributor. Off-net users include those connected through Media Gateway Control Protocol (MGCP)/skinny gateways, IOS H.323 gateways and IOS Media Gateway Control Protocol gateways. The Music On Hold feature is also available for Cisco IP POTS phones connected to the Cisco IP network through FXS ports on IOS H.323/Media Gateway Control Protocol and for Cisco Media Gateway Control Protocol/skinny gateways.

The integrated Music On Hold feature covers media server, data base administration, call control, media resource manager, and media control functional areas.

The music on hold server provides the music resources/streams. These resources register with the Cisco CallManager during the initialization/recovery period.

Database administration provides a user interface to allow the Cisco CallManager administrator to configure the Music On Hold feature for the device(s). Database administration also provides Cisco CallManager call control with configuration information.

Call control controls the music on hold scenario logic.

The media resource manager processes the registration request from the music on hold server and allocates/deallocates the music on hold resources under the request of call control.

Media control controls the establishment of media stream connections, which can be one-way or two-way connections.

An end device must be provisioned with music on hold-related information before music on hold functions for that device. Initializing a Cisco CallManager creates a media resource manager. The music on hold server(s) registers to the media resource manager with its music on hold resources.

When an end device or feature places a call on hold, Cisco CallManager connects the held device to a music resource. When the held device is retrieved, it disconnects from the music on hold resource and resumes normal activity.

Music On Hold Functionality

For music on hold to function, you must perform the actions in the following list:

- Configure music on hold servers.
- Configure audio sources.

Note Define audio sources first and then set up the music on hold servers, especially when multicast will be used. The user interface allows either step to take place first.

- Configure media resource groups. If multicast is desired, check the Use Multicast for MOH Audio check box.
- Configure media resource group lists.
- Assign media resource group lists and audio sources to device pools.
- Assign media resource group lists and audio sources to devices (to override assignments made to device pools).
- Assign audio sources to lines (to override device settings).

Using the preceding configuration actions, if you define music on hold functionality as follows, the examples that follow demonstrate music on hold functionality for user hold, transfer hold, and call park.

Media Resource Groups

MOH designates a music on hold server. MRG designates a media resource group.

- MRG_D comprises MOH_D.
- MRG_S_D comprises MOH_S and MOH_D.

Media Resource Group Lists

MRGL designates a media resource group list.

- MRGL_D comprises MRG_D.
- MRGL_S_D comprise MRG_S_D and MRG_D (prioritized order).

Nodes

- Dallas node comprises phone D and MOH_D.
- San Jose node comprises phone S and MOH_S.
- Assign phone D audio source ID 5, *Thank you for holding* (for both user and network hold), and MRGL_D.
- Assign phone S audio source ID 1, *Pop Music 1* (for both user and network hold), and MRGL_S_D.

User Hold Example

Phone D calls phone S, and phone S answers. Phone D presses the Hold softkey. Result: Phone S hears *Thank you for holding* streaming from MOH_S. (MOH_S has available streams.) When phone D presses the Resume softkey, phone S disconnects from the music stream and reconnects to phone D.

Transfer Hold Example

Transfer hold serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone D presses the Transfer softkey. Phone S hears *Thank you for holding* streaming from MOH_D. (MOH_S has no available streams, while MOH_D does.) After phone D completes the transfer action, phone S disconnects from the music stream and gets redirected to phone X, the transfer destination.

Call Park Example

Call park serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone S presses the CallPark softkey. Phone D hears a beep tone. (MOH_D has no available streams.) Phone X picks up the parked call. Phone S is redirected to phone X (phone D and phone X are conversing).

Supported Music On Hold Features

Music on hold supports the following features, which are listed by category. Feature categories include music on hold server characteristics, server scalability, server manageability, server redundancy, database scalability, and manageability.

Music On Hold Server Characteristics

- Servers stream music on hold from music on hold data source files stored on their disks.
- Servers stream music on hold from an external audio source (for example, looping tape recorder, radio, or CD).
- Music on hold servers can use a single music on hold data source for all source streams, and hence all connected streams. When multiple music on hold servers are involved, the local server of each music on hold server always stores the music on hold data source files. Cisco CallManager does not support distribution of fixed-device (hardware) audio sources across music on hold servers within a media resource group.
- Music on hold data source files have a common filename across all music on hold servers in a media resource group.
- Music on hold data source files are installed once and TFTPed as needed.
- Each audio source receives a feed from either a designated file or a designated fixed source (for example, radio or CD).
- A designated fixed source comprises a single device, which is either enabled or disabled.
- The audio driver on the local machine makes a single fixed source available to the music on hold server.
- Music on hold servers support the G.711 (a-law and mu-law), G.729a, and wideband codecs.
- Music on hold servers register with one primary Cisco CallManager server.

Server Scalability

- Music on hold supports from 1 to more than 500 simplex unicast streams per music on hold server.
- Music on hold supports multiple Cisco-developed media processing applications, including Interactive Voice Response (IVR) and AutoAttendant (AA). Cisco CallManager facilitates this support.
- Music on hold server simultaneously supports up to 50 music on hold data source files as sources.
- Music on hold server supports one fixed-device stream source in addition to the file stream sources.

Server Manageability

- You can install music on hold server application on any standard media convergence server (MCS) as a plugin from Cisco CallManager Administration windows.
- You can install music on hold application on the same media convergence server as other media applications, so that music on hold and the other media application(s) co-reside on the media convergence server.
- You can install music on hold server application on multiple media convergence servers in a cluster.
- The administrator can specify the source for each source stream provided by the server.
- Administration of stream sources takes place through a browser.

Server Redundancy

- Music on hold servers support Cisco CallManager lists. The first entry on the list serves as the primary server, and subsequent Cisco CallManagers on the list serve as backup Cisco CallManagers in prioritized order.
- Music on hold servers can maintain a primary and backup connection to Cisco CallManagers from their Cisco CallManager list.
- Music on hold servers can re-home to backup Cisco CallManagers following the standard procedures used by other servers and phones on the cluster.
- Music on hold servers can re-home to their primary server following standard procedures for other media servers on the cluster.

Cisco CallManager/Database Requirements

- When a Cisco CallManager is handling a call and places either endpoint in the call on hold, the Cisco CallManager can connect the held endpoint to music on hold. This feature holds true for both network hold and user hold. Network hold includes transfer, conference, call park, and so forth.
- A media resource group for music on hold supports having a single music source stream for all connected streams.
- The system supports having music on hold server(s) at a central site and no music on hold server(s) at remote sites. Remote site devices requiring music on hold service can obtain service from media resource group across the WAN when service is not available locally.
- You can distribute music on hold servers to any site within a cluster.
- A music on hold server can use a single music on hold data source for all source streams and, hence, all connected streams. When multiple music on hold servers are involved, the music on hold data source may be a file stored locally on each server.
- The system can detect when the primary media resource group that supplies music on hold for a device is out of streams and can select a stream from the secondary or tertiary media resource group specified for that device.
- When connecting a device to music on hold, the system can insert a transcoder when needed to support low-bandwidth codecs.

Database Scalability

- Cisco CallManager can support from 1 to more than 500 unicast sessions per music on hold server.
- A cluster can support from 1 to more than 20 music on hold servers.
- A cluster can support from 1 to more than 10,000 simultaneous music on hold streams across the cluster.
- A music on hold stream may be for hold.
- A music on hold stream may be for music on consult.
- A media resource group for music on hold can support from 1 to more than 10,000 simultaneous music on hold streams.
- A media resource group for music on hold may be for hold.
- A media resource group for music on hold may be for music on consult.

- A cluster can support from 1 to >= 500 media resource groups for music on hold.
- A media resource group for music on hold can support from 1 to >= 20 music on hold servers.

Manageability

- The administrator can select media resource group list per device.
- The administrator can select music on hold source stream per device/DN.
- The administrator can select music on consult (network hold) source stream per device/DN.
- The administrator can configure which music on hold servers are part of a specified media resource group.
- The administrator can designate a primary, secondary, and tertiary music on hold/consult servers for each device by configuring media resource groups and media resource group lists.
- The administrator can provision multiple music on hold servers.
- The administrator can provision any device registered with the system such that any music on hold server can service it in the system.
- All music on hold configuration and administration take place through a browser.
- Media resource groups for music on hold have a name.
- By including at least one music on hold server in each media resource group, the administrator creates all media resource groups that supply music on hold.
- The administrator specifies the user hold and network hold audio sources for each device pool. These default audio sources may be either file-based or fixed device-based.
- The administrator can designate a music on hold server as either unicast or multicast, provided that resources exist to support multicast.
- The administrator can reset all music on hold servers.

Music On Hold Server

The music on hold server uses the Station Stimulus (Skinny Client) messaging protocol for communication with Cisco CallManager. A music on hold server registers with the Cisco CallManager as a single device, reporting the number of simplex, unicast audio streams it can support. The music on hold server advertises its media type capabilities to the Cisco CallManager as G.711 mu-law and a-law, G.729, and wideband. Cisco CallManager starts and stops music on hold unicast streams by sending skinny client messages to the music on hold server.

A music on hold server handles up to 500 simplex, unicast audio streams. A media resource group includes one or more music on hold servers. A music on hold server supports 51 audio sources, with one audio source sourced from a fixed device using the local computer audio driver and the rest sourced from files on the local music on hold server.

You may use a single file for multiple music on hold servers, but the fixed device may be used as a source for only one music on hold server. The music on hold audio source files are stored in the proper format for streaming.
Cisco CallManager allocates the simplex unicast streams among the music on hold servers within a cluster.

The music on hold server uses the media convergence server series hardware platform. A sound card installed on the same computer as the music on hold server application provides the external audio source, which can be a looping tape recorder, radio, or CD.

The music on hold server, which is actually a component of the IP voice media streaming application, supports standard device recovery and database change notification.

The music on hold server uses the following DirectShow filters: fxcode.ax, ipvmsrend.ax, mohencode.ax, and wavdest.ax.

The music on hold server includes a hard-coded, read-only audio source storage directory. Do not change files in this directory, C:\Program Files\Cisco\MOH, in any way and do not add files to this directory.

Audio Sources for Music On Hold

An audio translator service converts administrator-supplied audio sources to the proper format for the music on hold server to use. The audio translator uses two parameters, an input directory and an output directory. You can configure the input directory, which defaults to C:\Cisco\DropMOHAudioSourceFilesHere, on a per-service basis. The output directory, a service-wide parameter, contains a Universal Naming Convention (UNC) name to a shared directory on the default MOH TFTP directory. For whatever directory is specified, \MOH is appended.

When the administrator drops an audio source file into the input directory, Cisco CallManager processes the file and then moves it into the output directory along with any generated files. Cisco CallManager supports most audio source file formats as input sources, including wav and mp3 files. After the input audio source is converted, an audio source file exists for each codec type that the music on hold server supports. Supply the highest quality source that is available.

Music On Hold CD-ROM

Cisco CallManager includes a default music on hold sample that automatically downloads with Cisco CallManager software for customer use.

In addition, a Music On Hold CD-ROM is available from Cisco. This CD-ROM contains other music and voice prompts designed for use with the Music On Hold feature. As a Cisco CallManager user, you are free to use any of the contents of this CD-ROM with MOH. Due to licensing restrictions, you may not distribute this music to anyone else, nor may you use it for any other purpose.

All music samples and voice prompts on the CD-ROM are 16-bit PCM sampled at 16 KHz. All samples and prompts can play with good audio quality in 7960/7940 wideband mode. If converted to G.711 format, some deterioration in audio quality may occur.

The music on hold CD-ROM contains the following types of music and voice prompts:

- ready-to-use MOH loops
- ready-to-use music
- ready-to-use voice prompts

Creating Audio Sources

When the music on hold server downloads audio source files, the \Program Files\Cisco\MOH directory stores the files. Do not manipulate this directory in any way: if files are updated or placed in this directory, they will be overwritten or ignored.

Most standard wav and mp3 files serve as valid input audio source files.

In creating an audio source, the following sequence takes place:

- The user places the audio source into the proper processing directory. Cisco CallManager automatically detects and translates the file. The output files and source files move into the directory on the Default MOH TFTP server holding directory. This holding directory comprises the DefaultTFTPMOHFilePath with \MOH appended. Conversion of a 3-MB mp3 file or a 21-MB wav file takes approximately 30 seconds.

Warning **If the audio translator translates audio source files on the same server as the Cisco CallManager, serious problems may occur. The audio translator tries to use all available CPU time, and Cisco CallManager may experience errors or slowdowns. Make sure audio translation never takes place on an active Cisco CallManager.**

- When the user assigns or maps the audio source file to an audio source number, the proper audio source files are copied to a directory one level higher in the directory structure to make them available for the music on hold servers.
- The music on hold servers download the needed audio source files and store them in the hard-coded directory C:\Program Files\Cisco\MOH.
- The music on hold server then streams the files using DirectShow and the kernel mode RTP driver as needed or requested by Cisco CallManager.

Managing Audio Sources

Once music on hold audio sources are created, their management occurs entirely through the Cisco CallManager Administration web interface. Choose **Service > Music On Hold** to display the Music On Hold (MOH) Audio Source Configuration window. For a given audio source, use this window to add, copy,

update, or delete a music on hold audio source. For each audio source file, assign a music on hold audio source number and music on hold audio source name and decide whether this audio source will play continuously and allow multicasting. For an audio source, this window also displays the music on hold audio source file status. Refer to "Configuring Music On Hold Audio Sources" in the *Cisco CallManager Administration Guide* for details.

Multicast and Unicast Audio Sources

Multicast music on hold conserves system resources. Multicast allows multiple users to use the same audio source stream to provide music on hold. Multicast audio sources are associated with an IP address.

Unicast music on hold, the system default, uses a separate source stream for each user or connection. Users connect to a specific device or stream.

For administrators, multicast entails managing devices, IP addresses, and ports. In contrast, unicast entails managing devices only.

For multicast, administrators must define at least one audio source to allow multicasting. To define music on hold servers for multicast, first define the server to allow multicasting.

Devices request a multicast connection by using either an IP address or a port number. The default specifies a port number. In firewall situations, because an IP address is preferable, administrators should choose to increment multicast by IP address.

The Max Hops field in the Music On Hold (MOH) Server Configuration window indicates the maximum number of routers that an audio source is allowed to cross. If max hops is set to zero, the audio source must remain in its own subnet. If max hops is set to one, the audio source can cross up to one router to the next subnet. Cisco recommends setting max hops to two.

A standards body reserves IP addresses. Addresses for IP multicast range from 224.0.1.0 to 239.255.255.255. The standards body, however, assigns addresses in the range 224.0.1.0 to 238.255.255.255 for public multicast applications. Cisco strongly discourages using public multicast addresses for music on hold multicast. Instead, Cisco recommends using an IP address in the range reserved for administratively controlled applications on private networks (239.0.0.0 to 239.255.255.255).

Valid port numbers for multicast include even numbers that range from 16384 to 32767. (Odd values are reserved.)

Multicast functions only if both media resource groups and media resource group lists are defined to include a multicast music on hold server. For media resource groups, you must include a music on hold server that is set up for multicast. Such servers are labeled as *(MOH)[Multicast]*. Also, check the Use Multicast for MOH Audio check box when defining a media resource group for multicast.

For media resource group lists, which are associated with device pools and devices, define the media resource group list so that the media resource group set up for multicast is the first group in the list. This recommended practice facilitates the device efforts to find the multicast audio source first.

In music on hold processing, the held device (the device placed on hold) determines the media resource to use, but the holding device (the device that initiates the hold action) determines the audio source to use.

Multicast Configuration Checklist

Table 19-1 provides a checklist for configuring various Cisco Call Manager services to allow multicasting. All steps must be performed in order for multicast to be available.

Table 19-1 Multicast Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Configure an audio source to allow multicasting.	Music On Hold Audio Source Configuration Settings, *Cisco CallManager Administration Guide*
Step 2	Configure a music on hold server to enable multicast audio sources.	Music On Hold Server Configuration Settings, *Cisco CallManager Administration Guide*
Step 3	Create a media resource group and configure it to use multicast for MOH audio.	Media Resource Group Configuration Settings, *Cisco CallManager Administration Guide*
Step 4	Create a media resource group list with a multicast media resource group as the primary media resource group.	Media Resource Group List Configuration Settings, *Cisco CallManager Administration Guide*
Step 5	Select the media resource group list created in Step 4 for either a device pool or for specific devices.	Device Pool Configuration Settings, *Cisco CallManager Administration Guide*

Music On Hold System Requirements and Limits

The following system requirements and limits apply to the Music On Hold feature:

- All audio streaming devices using the Music On Hold feature support simplex streams. The music on hold server supports at least 500 simplex streams.
- The music on hold server, which is installed as an option from Cisco CallManager Administration, can coexist with other Cisco and third-party media applications. Only one music on hold server may be

installed on a media convergence server, but the music on hold server may be installed on multiple media convergence servers. The music on hold server is installed as part of the IP Voice Media Streaming application.

- For each music on hold audio server, you may define up to 50 audio sources. A Cisco CallManager Administration web page supports addition, update, and deletion of each audio source. The music on hold server also supports one fixed input source. The following codecs are supported: G.711 a-law/mu-law, G.729a, and wideband.
- For each cluster, you may define up to 50 audio sources from files as well as one fixed audio source. A Cisco CallManager Administration web page supports addition, update, and deletion of each audio source. All servers use local copies of the same 50 or fewer files. You must set up the fixed audio source that is configured per cluster on each server.
- For each cluster, you may define at least 20 music on hold servers. The Cisco CallManager Administration web page allows addition, update, and deletion of music on hold servers. The web page allows administrators to specify the following characteristics for each server:
  - Name
  - Node (server host name)
  - Device pool
  - Maximum number of unicast and multicast streams
  - Sources to multicast
  - For each multicast source: IP address, port, and time to live (maximum number of router hops)
- Cisco CallManager Administration allows definition of at least 500 media resource groups per cluster. Each media resource group may include any combination of at least 20 media resources, including music on hold servers, media termination points, transcoders, and conference devices. Music on hold servers in one cluster support at least 10,000 simultaneous music on hold streams. See Media Resource Groups, page 16-4, for details of media resource groups.
- Cisco CallManager Administration allows definition of media resource group lists. See Media Resource Group Lists, page 16-5, for details of media resource group lists.

- Modifications to the Cisco CallManager Administration device configuration windows for phones and gateways allow the selection of a media resource group list, hold stream source, and consult stream source. These parameters are optional for a device.
- Modifications to the Cisco CallManager Administration Directory Number configuration windows allow selection of a hold stream source and a consult stream source.
- Modifications to the Cisco CallManager Administration Service Parameters allows entry to a service-wide, default music on hold stream source (default is 1) and default media resource group type (default is unicast).
- The Music On Hold feature does not use nor require computer telephony integration (CTI), java telephony application programmer interface (JTAPI), telephony application programmer's interface (TAPI), or any other third-party application.
- The Music On Hold feature does not use firmware.
- The number of streams that the music on hold server can use may decrease if the TAPI wav driver, software MTP, or software conference bridge is in use on the same MSC server.

Music On Hold Failover and Failback

The music on hold server supports Cisco CallManager lists and failover as implemented by the software conference bridge and media termination point. Upon failover, connections to a backup Cisco CallManager are maintained if one is available.

Cisco CallManager takes no special action when a music on hold server goes down during an active music on hold session. The held party hears nothing from this point, but this situation does not affect normal call functions.

Music On Hold Configuration Checklist

Table 19-2 provides a checklist for configuring music on hold.

Table 19-2 Music On Hold Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Install music on hold using the installation CD. Select the Cisco IP Voice Media Streaming application. The Audio Translator is installed at the same time. Cisco CallManager automatically adds the media termination point, conference bridge, and music on hold devices to the database. When the services are registered, the DirectShow filters automatically install and register. **Note** During installation, Cisco CallManager installs and configures a default music on hold audio source if one does not exist. Music on hold functionality can proceed using this default audio source without any other changes.	*Installing Cisco CallManager Release 3.1*
Step 2	Run the music on hold audio translator. **Warning** **If the audio translator translates files on the same server as the Cisco CallManager, serious problems may occur. The audio translator tries to use all available CPU time, and Cisco CallManager may experience errors or slowdowns.**	Audio Sources for Music On Hold, page 19-12
Note	The installation program performs the following actions automatically. If the user manually adds the music on hold components, the following steps are necessary.	
Step 3	Configure the music on hold server.	Configuring Music On Hold Servers, *Cisco CallManager Administration Guide*

Table 19-2 Music On Hold Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 4	Add and configure audio source files.	Configuring Music On Hold Audio Sources, *Cisco CallManager Administration Guide*
Step 5	Configure the fixed audio source.	Configuring the Music On Hold Fixed Audio Source, *Cisco CallManager Administration Guide*

Monitoring Music On Hold Performance

Perform the activities in Table 19-3 to monitor and troubleshoot music on hold performance.

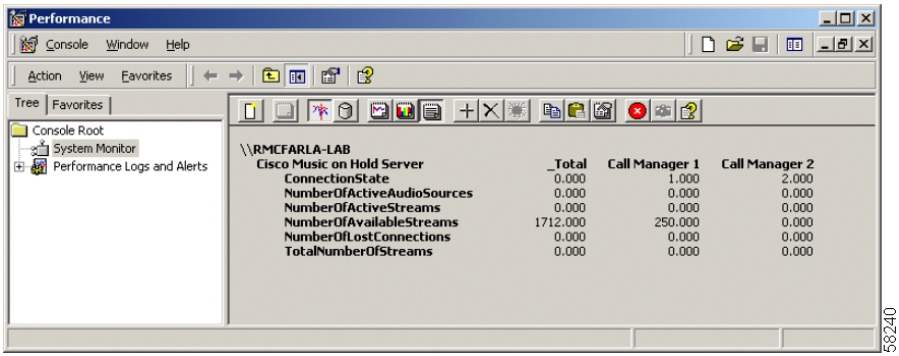
Table 19-3 Music On Hold Performance Monitoring and Troubleshooting

Monitoring/Troubleshooting Activity		Detailed Information
Step 1	Use perfmon to check resource usage and device recovery state.	Refer to "Viewing Music On Hold Server Perfmon Counters" section on page 19-21 for details. *Cisco CallManager Serviceability Administration Guide* documents another method of viewing this information.
Step 2	Search the event log for Cisco IP Voice Media Streaming application entries.	Refer to the *Cisco CallManager Serviceability Administration Guide* for details.
Step 3	Verify that service driver is running.	Refer to "Checking Service States" section on page 19-22 for details. *Cisco CallManager Serviceability Administration Guide* documents another method of viewing this information.
Step 4	Verify that device driver is running.	Refer to "Checking Device Driver States" section on page 19-23 for details.
Step 5	Search the Media Application trace to see what music on hold-related activity it detects.	Refer to the *Cisco CallManager Serviceability Administration Guide* for details.

Viewing Music On Hold Server Perfmon Counters

To view music on hold server perfmon counters, access the Performance window by choosing **Administrative Tools > Performance > Console Root > System Monitor**. The Performance window displays. Figure 19-1 provides an example.

Figure 19-1 Performance Window Example



This window shows all the Cisco music on hold server performance counters. The Cisco CallManager has its own performance counters that pertain to music on hold. Table 19-4 details the performance counters displayed in the Performance window.

Table 19-4 Music On Hold Performance Counters

Performance Counter Name	Description
ConnectionState	Indicates primary and secondary Cisco CallManager: • 1 = Primary • 2 = Secondary • 0 = Not connected
NumberOfActiveAudioSources	Specifies total number of active audio sources, including each supported codec type. If audio Source 1 has mu-law and G.729 enabled, count for this audio source may be 2.

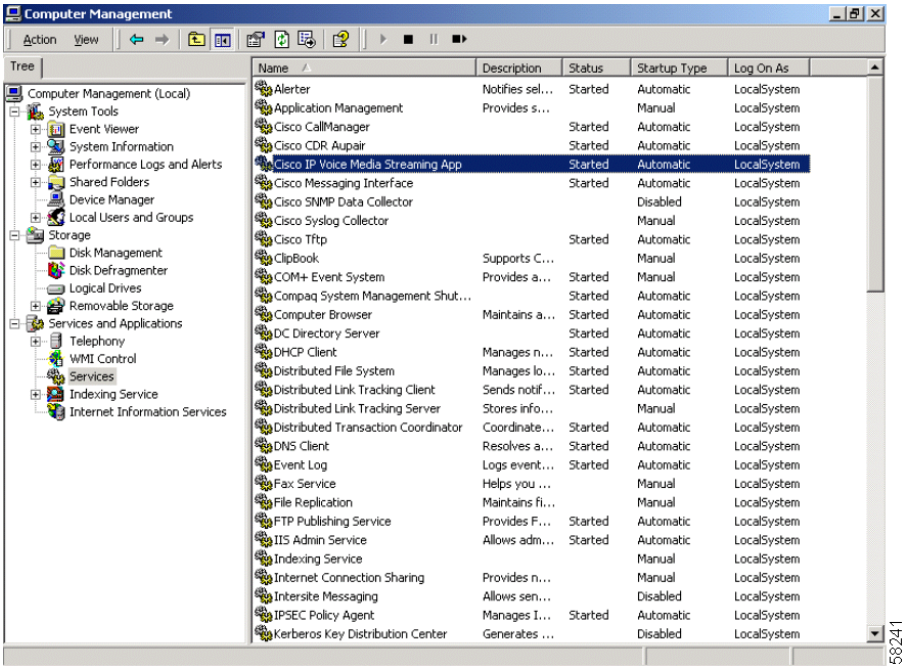
Table 19-4 Music On Hold Performance Counters (continued)

Performance Counter Name	Description
NumberOfActiveStreams	Specifies total number of active streams. Two potential overhead streams exist for each audio source/codec type: one for actual audio source, another for multicast.
NumberOfAvailableStreams	Specifies total number of available simplex streams. Total represents total number of available streams in device driver for all devices.
NumberOfLostConnections	Specifies number of times connection has been lost for the corresponding Cisco CallManager.
TotalNumberOfStreams	Specifies total number of streams processed.

Checking Service States

To check whether the music on hold service is running, display the Computer Management (Services) window by choosing **Computer Management > Services and Applications > Services**. The Computer Management window displays a list of services and applications. Figure 19-2 provides an example.

Figure 19-2 Computer Management (Services) Window Example

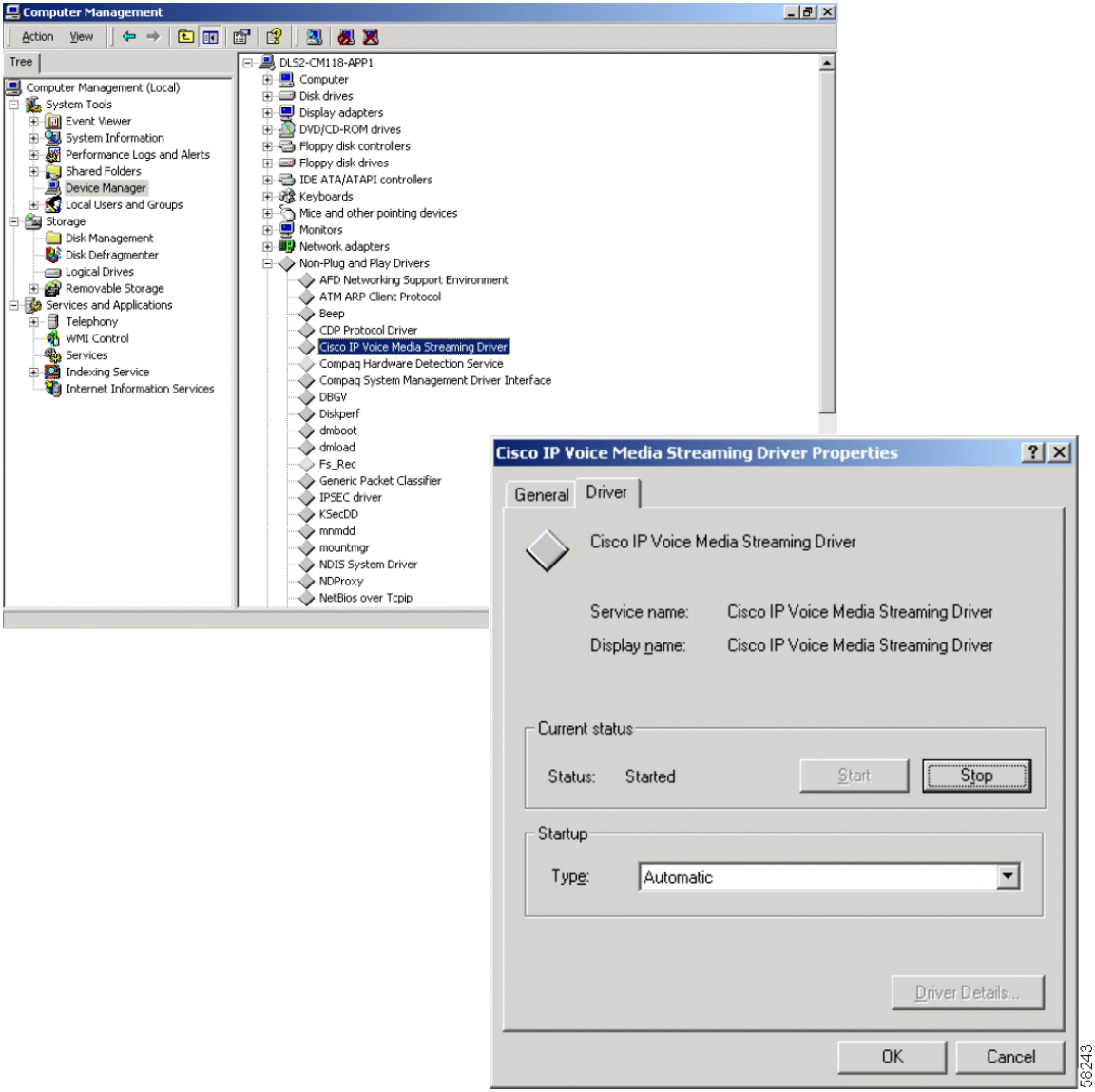


Search this window for a *Cisco IP Voice Media Streaming App* entry. If the service is running, its state should be *Started*.

Checking Device Driver States

To check whether the device driver is running, display the Computer Management (Device Manager) window by choosing **Computer Management > System Tools > Device Manager**. The Computer Management window displays. Figure 19-3 provides an example.

Figure 19-3 Computer Management Window (Device Driver) Example



Right-click a driver and choose its properties to view an expanded driver view. Look at the Current status field for a Status of *Started*. To view non-plug-and-play drivers, choose **Device Manager > View/Show hidden devices**.

Where to Find More Information

Additional Cisco Documentation

- Music On Hold Configuration, *Cisco CallManager Administration Guide*
- Media Resource Group Configuration, *Cisco CallManager Administration Guide*
- Media Resource Group List Configuration, *Cisco CallManager Administration Guide*
- *Installing Cisco CallManager Release 3.1*
- *Upgrading Cisco CallManager Release 3.1*
- *Cisco CallManager Serviceability Administration Guide*

CHAPTER 20

Media Termination Points

A Media Termination Point (MTP) software device allows the Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

This section covers the following topics:

Understanding Media Termination Points

The MTP accepts two full duplex G.711 Coder-Decoder (CODEC) stream connections. MTPs bridge the media streams between two connections. The streaming data received from the input stream on one connection is passed 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.

MTPs 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.

Each MTP belongs to a device pool, which specifies the list of Cisco CallManagers, in priority order, to which the devices that are members of the device pool should attempt to register. This list is called a Cisco CallManager group. The first Cisco CallManager in the list is a device's primary Cisco CallManager.

An MTP device always registers with its primary Cisco CallManager if that Cisco CallManager is available and informs the Cisco CallManager about how many MTP resources it supports. The Cisco CallManager controls MTP resources. Multiple MTPs may be registered with the same Cisco CallManager. When more than one MTP is registered with a given Cisco CallManager, that Cisco CallManager controls the set of resources for each of the MTPs. The MTPs can also be distributed across a networked system as desired.

For example, MTP server 1 is configured for 48 MTP resources. The MTP server 2 is configured for 24 resources. If both MTPs register with the same Cisco CallManager, that Cisco CallManager maintains both sets of resources for a total of 72 registered MTP resources.

When the Cisco 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 is inserted into the call on behalf of the endpoint. MTP resource use is invisible to both the users of the system, and 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 supplementary services are not available on that call.

Make sure the Cisco IP Voice Media Streaming application is installed and running on the server on which the MTP device is configured.

The Cisco IP Voice Media Streaming application is common to both the MTP, Conference Bridge, and Music On Hold applications. The application runs as a service within Windows 2000.

You can add an MTP device in two ways:

- An MTP device is automatically added if you choose to install the optional component called "Cisco IP Voice Media Streaming Application" during the automated installation of Cisco CallManager.
- 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 CallManager Administration.

Managing MTPs with the Media Resource Manager

The Media Resource Manager (MRM) is a software component in the Cisco CallManager system. The MRM primary functions are resource registration and resource reservation. Each MTP device defined in the database registers with the MRM. The MRM keeps track of the total available MTP devices in the system and which devices have available resources.

During resource reservation, the MRM determines the number of resources, identifies the media type (in this case, the MTP), and the location of the registered MTP device. The MRM updates its share resource table with the registration information and propagates the registered information to the other Cisco CallManagers within the cluster.

The MRM enhances the Cisco CallManager MTP, Music On Hold, Conference Bridge, and Transcoder devices by distributing the resources throughout the CallManager cluster, making the features more efficient and economical.

MRM also supports the co-existence of an MTP and transcoder within a Cisco CallManager.

Planning Your MTP Configuration

One of the most crucial aspects that need consideration when deploying MTP resources is provisioning, which requires attentive analysis of the call load patterns and the network topology.

Consider the following information when 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) card. 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 available depends on the amount of resources being consumed by other applications on that PC, the speed of the processor, network loading, and various other factors.

  Consider the following formula to determine the approximate number of MTPs needed for your system, assuming that your server can handle 48 MTP resources (you can substitute 48 for the correct number of MTP resources supported by your system):

  A divided by 48 = number of MTP applications needed (*n*/48 = number of MTP applications).

  where:

  n represents the number of H.323 devices that require MTP support.

  If a remainder exists, add another server with Cisco IP Voice Streaming Application server with MTP.
- If one H.323 endpoint requires an MTP, it consumes one MTP resource. Depending on the originating and terminating device type, more than one MTP resource might be consumed by a given call. The MTP resources assigned to the call are released when the call is terminated.

- Use Performance Monitor to monitor the usage of MTP resources. The Performance Monitor counter, Media TermPoints Out of Resources, increments for each H.323 call that has been connected 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.
- The system requirements for the Cisco IP Voice Media Streaming Application and MTP are the same as Cisco CallManager system requirements.

MTP Device Characteristics

The Full Streaming Endpoint Duplex Count, a number of MTP resources supported by a specific MTP, is a device characteristic that is specific to MTP device configuration. Refer to the "Media Termination Configuration Settings" section in the *Cisco CallManager Administration Guide* for a detailed description of all MTP device settings.

Avoiding Call Failure/User Alert

Avoid the following conditions to prevent call failure or user alert:

- Although the Cisco IP Voice Media Streaming Application service can be installed on the same PC as the Cisco CallManager, we strongly recommend against this. If the Cisco IP Voice Media Streaming Application is installed on the same PC as the Cisco CallManager, it can adversely affect the performance of the Cisco CallManager.
- When you configure the MTP, you are prompted to reset MTP before any changes can take effect. This does not result in disconnection of any calls 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 connected to the MTP are dropped.

MTP System Requirements and Limitations

The following system requirements and limitations apply to MTP devices:

- Only one Cisco IP Voice Streaming Application can be installed per server. To provide more MTP resources, you can install the Cisco IP Voice Streaming application on additional networked Windows NT servers.
- Each MTP can register with only one Cisco CallManager at a time. The system may have multiple MTPs, each of which may be registered to one Cisco CallManager, depending on how your system is configured.
- It is strongly recommended that the Cisco IP Voice Streaming Media Application *not* be installed on a Cisco CallManager with a high call processing load, because it can adversely affect the performance of the Cisco CallManager.

MTP Failover and Failback

This section describes how MTP devices failover and failback in the event that the Cisco CallManager to which they are registered becomes unreachable. Conditions that can affect calls associated with an MTP device, such as MTP reset or restart, are also explained.

Active Cisco CallManager Becomes Inactive

The following describes the MTP device recovery methods when the MTP is registered to a Cisco CallManager that goes inactive.

- If the primary Cisco CallManager fails, the MTP attempts to register with the next available Cisco CallManager in the Cisco CallManager Group specified for the device pool to which the MTP belongs.
- The MTP device re-registers with the primary Cisco CallManager as soon as it becomes available after a failure, and is currently not in use.

- An MTP device is registered to a Cisco CallManager that becomes unreachable. The calls or conferences that were on that Cisco CallManager will register with the next Cisco CallManager in the list.
- If an MTP attempts to register with a new Cisco CallManager and the register acknowledgment is never received, the MTP registers with the next Cisco CallManager.

Resetting Registered MTP Devices

The MTP devices will un-register and then disconnect after a hard or soft reset. After the reset completes, the devices re-register with the Cisco CallManager.

MTP Configuration Checklist

Table 20-1 provides a checklist to configure MTP.

Table 20-1 MTP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Determine the number of MTP resources needed and the number of MTP devices needed to provide these resources.	Planning Your MTP Configuration, page 20-4
Step 2	Verify that the Cisco IP Voice Media Streaming Application service is installed and running on the server to which you are adding an MTP.	*Cisco CallManager Serviceability Administration Guide*
Step 3	Add and configure the MTPs.	Adding a Media Termination Point, *Cisco CallManager Administration Guide*
Step 4	Add the new MTPs to the appropriate Media Resource groups.	Chapter 16, "Media Resource Management" Media Resource Group Configuration Settings, *Cisco CallManager Administration Guide*
Step 5	Restart the MTP device.	

Where to Find More Information

Related Topics

- Media Resource Management, page 16-1
- Transcoders, page 18-1

Additional Cisco Documentation

- Media Resource Group Configuration, *Cisco CallManager Administration Guide*
- Media Resource Group Configuration Settings, *Cisco CallManager Administration Guide*
- *Cisco IP Telephony Network Design Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network/

CHAPTER 21

Catalyst DSP Resources for Transcoding and Conferencing

This chapter describes Catalyst digital signal processor (DSP) resources and how they are used for transcoding and conferencing. The modules include the WS-X4604-GWY for the Catalyst 4000 and the WS-X6608-T1 (WS-X6608-E1 for countries outside the USA) for the Catalyst 6000. The modules, available for use with Cisco CallManager, can perform conferencing and Media Termination Point (MTP) transcoding services in addition to serving as a PSTN gateway.

This chapter covers the following topics:

Understanding Catalyst DSP Resources

The DSP resources on the new Catalyst 4000 and 6000 gateway modules essentially provide hardware support for IP telephony features offered by Cisco CallManager. These features include hardware-enabled voice conferencing, hardware-based MTP support for supplementary services, and transcoding services.

Catalyst-enabled *conferencing* designates the ability to support voice conferences in hardware. DSPs convert voice over IP (VoIP) sessions into time-division-multiplexing (TDM) streams, which can then be mixed into a multiparty conference call.

The Catalyst 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 using gateways and clients that do not support the H.323v2 feature of OpenLogicalChannel and CloseLogicalChannel with the EmptyCapabilitiesSet. MTP, available as a software feature, can run on Cisco CallManager or a separate Windows NT server. When MTP is running in software on Cisco CallManager, the resource supports 24 MTP sessions. When MTP is running on a separate Windows NT server, the resource supports up to 48 MTP sessions. The new Catalyst gateway modules can support this same functionality, but they provide the service in the hardware.

Transcoding in effect provides an IP-to-IP voice gateway service. A transcoding node can convert a G.711 voice stream into a low-bit-rate (LBR), compressed voice stream, such as G.729a. This is critical for enabling applications such as integrated voice response (IVR), voice messaging, and conference calls over low-speed IP WANs. MTP transcoding is currently supported only on the Catalyst voice gateways.

Table 21-1 shows DSP resources that can be configured on the Catalyst voice services modules.

Table 21-1 Catalyst DSP Resource Matrix

Catalyst Voice Modules	PSTN Gateway Sessions	Conferencing Sessions	MTP Transcoding Sessions
Catalyst 4000 WS-X4604-GWY	G.711 only • 96 calls	G.711 only • 24 conference participants • Maximum of 4 conferences of 6 participants each	To G.711 • 16 MTP transcoding sessions
Catalyst 6000 WS-6608-T1 or WS-6608-E1	WS-6608-T1 • 24 calls per physical DS1 port • 192 calls per module WS-6608-E1 • 30 calls per physical DS1 port • 240 calls per module	G.711 or G.723 • 32 conferencing participants per physical port • Maximum conference size of 6 participants • 256 conference participants per module G.729 • 24 conferencing participants per physical port • Maximum conference size of 6 participants • 192 conference participants per module	The following capacities also apply to simultaneous transcoding and conferencing: G.723 to G.711 • 31 MTP transcoding sessions per physical port • 248 sessions per module G.729 to G.711 • 24 MTP transcoding sessions per physical port • 192 sessions per module

DSP Resource Manager

The DSP resource management (DSPRM) maintains the state for each DSP channel and the DSP. A resource table is maintained for each DSP. The DSPRM is responsible for the following:

- Discover the on-board DSP simm modules and, based on the user configuration, determine the type of application image a DSP uses.
- Reset DSPs, bring up DSPs, and application image download to DSP.
- Maintains 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 PCI driver for sending and receiving DSP control messages.
- Handle failure cases, such as DSP crashes and session terminations.
- A keepalive mechanism between the DSPs and the primary, and backup, Cisco CallManagers. The primary Cisco CallManager can use this keepalive to determine when DSPs are no longer available.
- Perform periodic DSP resource checks.

Depending on user configuration, two DSP pools are maintained: one for transcoding and one for conferencing. When a request is received from the signaling layers for a session, the first available DSP from the respective pool is assigned along with the first available channel. A set of MAX limits (such as maximum conference sessions per DSP or maximum transcoding session per DSP) are maintained for each DSP.

Call Preservation

A switchover occurs when a higher order Cisco CallManager becomes inactive or the communication link between the DSPs and the higher order Cisco CallManager disconnects.

A switchback occurs when the higher order Cisco CallManager becomes active again and DSPs can switchback to the higher order Cisco CallManager.

When a switchover or switchback registration occurs, the DSPRM reports the number of active connections along with the number of RTP streams. Once the call disconnects, the DSPRM detects the media streaming failure by reacting to the ICMP "port not reachable" indications received on the RTP port and reports this information to the currently active Cisco CallManager using SCCPs new "StationMediaStreamingFailure" message. The Cisco CallManager can now update the status of the specified resource that becomes available for use in a new connection establishment. This method is called disconnect supervision.

Catalyst MTP Transcoding Services

Introducing the WAN into an IP telephony implementation forces the issue of voice compression. Once a WAN-enabled network is implemented, voice compression between sites represents the recommended design choice in order 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.

MTP Transcoding Design Details

The following points summarize the design capabilities and requirements of the MTP transcoding:

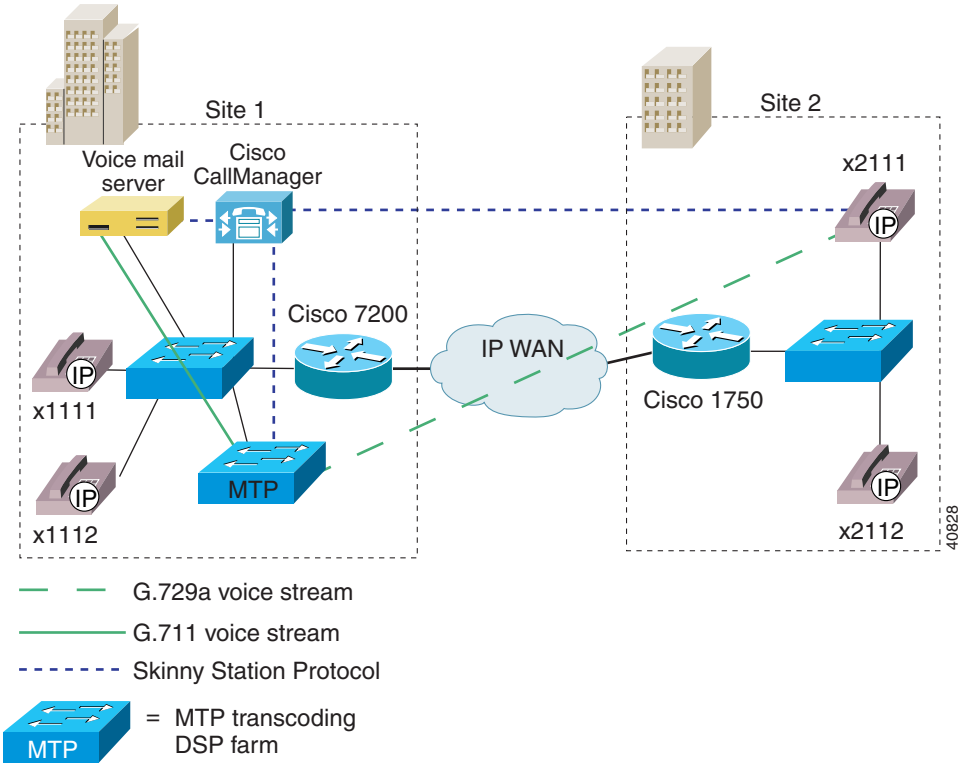
- Provision MTP transcoding resources appropriately for the number of IP WAN callers to G.711 endpoints.
- The Catalyst 4000 WS-X4604-GWY module supports 16 transcoding sessions per module.
- The Catalyst 6000 WS-X6608-T1 or WS-X6608-E1 modules support 31 G.723 or G.711 transcoding sessions per physical port (248 per module) or 24 G.729 to G.711 transcoding sessions per physical port (192 per module).
- Transcoding is supported only in low bit rate to high bit rate (G.729a or G.723.1 to G.711), or vice versa, configurations.

- Each Cisco CallManager must have its own MTP transcoding resources.
- Each transcode has its own jitter buffer of 20-40 ms.

IP-to-IP Packet Transcoding and Voice Compression

Voice compression between IP phones is easily configured through the use of regions and locations in Cisco CallManager. However, the 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 two of the new modules for the Catalyst 4000 and Catalyst 6000. A packet-to-packet gateway designates a device with DSPs that has the job of transcoding between voice streams using different compression algorithms. That is, when a user on an IP phone at a remote location calls a user at the central location, Cisco CallManager instructs the remote IP phone to use compressed voice, or G.729a, only for the WAN call. However, if the called party at the central site is unavailable, the call potentially rolls 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. See Figure 21-1.

Figure 21-1 IP-to-IP Packet Gateway Transcoding for the WAN with Centralized Call Processing

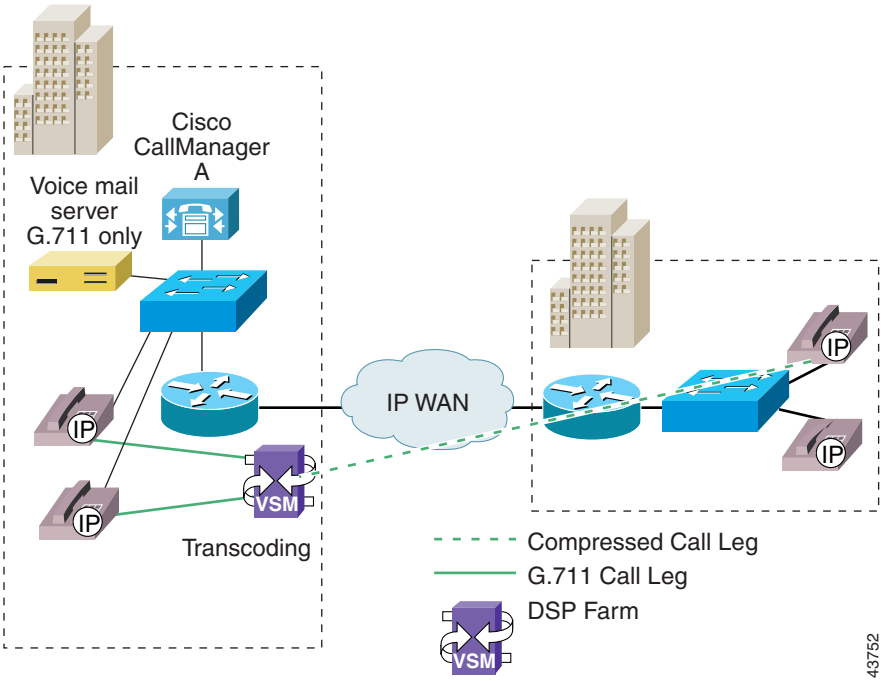


Voice Compression, IP-to-IP Packet Transcoding, and Conferencing

Connecting sites across an IP WAN for conference calls presents a complex scenario. In this scenario, the Catalyst modules must perform the conferencing service as well as the IP-to-IP transcoding service to uncompress the WAN IP voice connection. In Figure 21-2, 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 Catalyst 6000. The following list gives the channel usage:

- 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
- Catalyst 6000
  - Three conferencing DSP channels. On the Catalyst 6000, all voice streams are sent to single logical conferencing port where all transcoding and summing takes place.

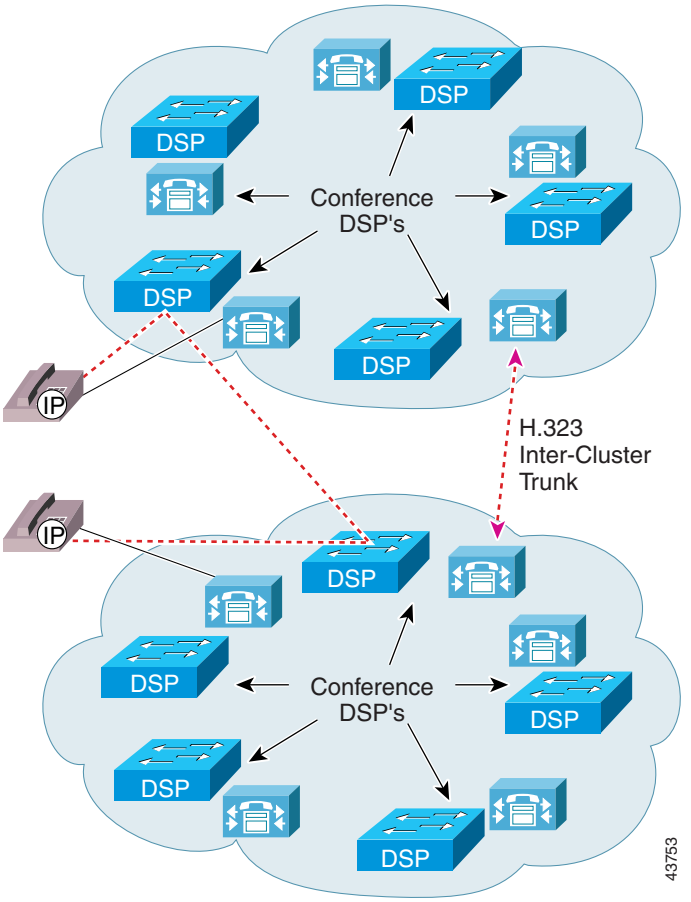
Figure 21-2 Multisite WAN Using Centralized MTP Transcoding and Conferencing Services



IP-to-IP Packet Transcoding Across Intercluster Trunks

H.323v2 intercluster trunks connect Cisco CallManager clusters. If transcoding services are needed between clusters, the intercluster trunks are configured with MTP. In this case, all calls between clusters route through the MTP/transcoding devices in each cluster. The Catalyst 6000 module uses the MTP service regardless whether transcoding is needed for that particular intercluster call. Cisco CallManager supports compressed voice call connection through the MTP service if a hardware MTP is used. Figure 21-3 shows an intercluster call flow.

Figure 21-3 Intercluster Call Flow with Transcoding



The following list gives intercluster MTP/transcoding details:

- If transcoding is required between Cisco CallManager clusters, you must configure the H.323 intercluster trunk with an MTP resource.
- All calls between Cisco CallManager clusters go through MTPs.
- Outbound intercluster calls will use an MTP/transcoding resource from the Cisco CallManager from which the call originates.
- Inbound intercluster call will use the MTP/resource from the Cisco CallManager that terminates the inbound intercluster trunk.
- Additional DSP MTP/transcoding resources should be allocated to Cisco CallManagers terminating H.323 intercluster trunks

Catalyst Conferencing Services

To scale IP telephony systems in large enterprise environments, you must use hardware-based conferencing. The new hardware for the Catalyst 4000 and 6000 switch families keeps this requirement in mind. These new Catalyst voice modules can handle conferencing in hardware, eliminating the requirement of running a software conferencing service on a Windows NT server in the IP telephony network.

Conferencing Design Details

The following points summarize the design capabilities and requirements of the new Catalyst voice modules:

- Support exists for a maximum of six participants per conference call.
- The Catalyst 4000 WS-X4604-GWY module supports 24 conference participants per module.
- The Catalyst 4000 WS-X4604-GWY module supports conferencing for G.711 voice streams only. Transcoding can convert G.729a or G.723.1 to G.711 for conference calls.
- The Catalyst 6000 WS-X6608-T1 or WS-X6608-E1 modules support 32 G.711 or G.723 conference participants per physical port (256 per module) or 24 G.729 conference participants per physical port (192 per module).

- The Catalyst 6000 WS-X6608-T1 or WS-X6608-E1 modules can support both uncompressed and compressed VoIP conference calls.
- Make sure each Cisco CallManager has its own conference and MTP transcoding resources because the DSP resources can register with only one Cisco CallManager at a time. Cisco CallManagers cannot share DSP resources.

The Catalyst 4000 module, the WS-X4604-GWY, can support up to four simultaneous conference calls of six callers each. The Catalyst 6000 T1 or E1 PSTN gateway module, the WS-X6608, also can support conferencing. After the WS-X6608 has been added as a T1 or E1 Cisco AVVID gateway, you can configure it, on a per-port basis, for conferencing services. The Catalyst 6000 conferencing module supports up to six callers per conference call with a maximum of 32 simultaneous G.711 or G.723 conference callers per configured logical port. This configuration results in a maximum of 256 conference participants per module with G.711 or G.723 calls.

See Table 21-1 for a summary of conference call densities for each module.

Both the WS-X4604-GWY and WS-X6608-T1 (or WS-X6608-E1) modules use Skinny Station Protocol to communicate with Cisco CallManager when providing conferencing or transcoding services. The Catalyst 6000 voice conferencing solution can support both compressed and uncompressed conference attendees.

On the Catalyst 4000, only G.711, or uncompressed, calls can join to a conference call. When the conferencing service registers with Cisco CallManager, using Skinny Station Protocol, it announces that only G.711 voice calls can connect. If any compressed calls request to be joined to a conference call, Cisco CallManager connects them to a transcoding port first, to convert the compressed voice call to G.711. Once the G.711 connections are associated with a particular conferencing session (maximum of six participants per conference call), the call converts to a TDM stream and passes to the summing logic, which combines the streams.

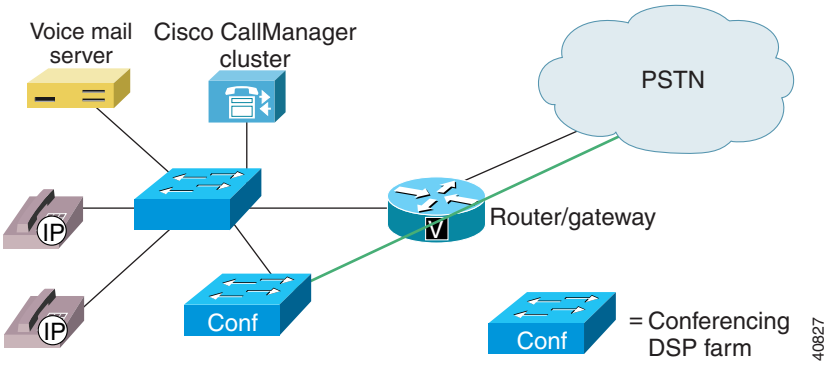
Unlike the WS-X6608-x1, which can mix all conference call participants, the Catalyst 4000 WS-X4604-GWY module sums only the three dominant speakers. The WS-X4604-GWY dynamically adjusts for the dominant speakers and determines dominance primarily by voice volume, not including any background noise.

You should also observe the following recommendations when configuring conferencing services:

- When provisioning an enterprise with conference ports, first determine how many callers will attempt to join the conference calls from a compressed Cisco CallManager region. Once you know the number of compressed callers, you can accurately provision the MTP transcoding resources.
- Conference bridges can register with more than one Cisco CallManager at a time, and Cisco CallManagers can share DSP resources through the Media Resource Manager (MRM).

Figure 21-4 illustrates the components used in Catalyst conferencing services.

Figure 21-4 Catalyst Conferencing Services



Catalyst 4000 Voice Services

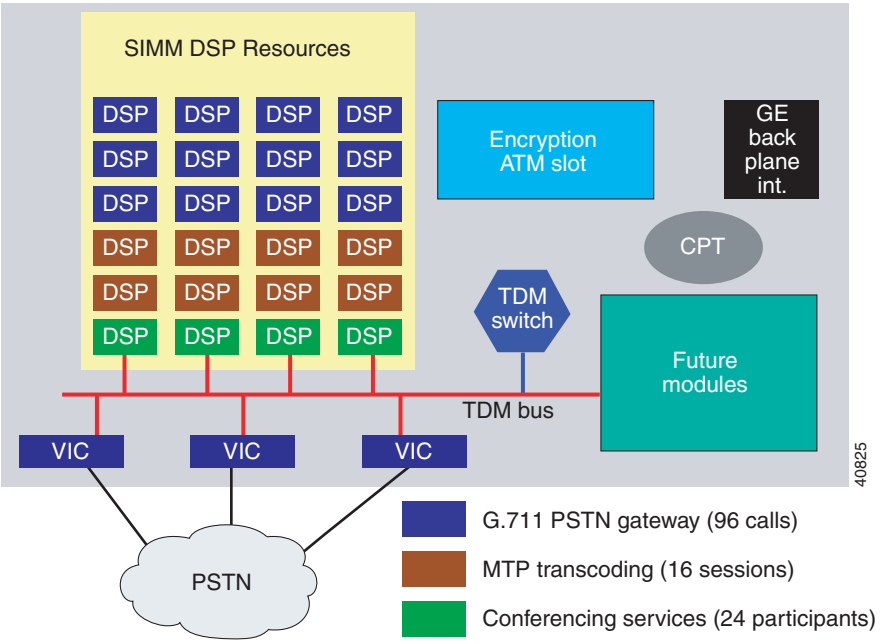
The PSTN gateway and voice services module for the Catalyst 4003 and 4006 switches supports three analog voice interface cards (VICs) with two ports each or one T1/E1 card with two ports and two analog VICs. Provisioning choices for the VIC interfaces any combination of Foreign Exchange Office (FXO), 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 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. Once the gateway mode is enabled, the module's 24 DSPs (4 SIMMs with 6 DSPs each) occurs as follows:

- PSTN gateway: 96 channels of G.711 voice *and*
- Conferencing: 24 channels of G.711 conferencing *and*
- MTP transcoding: 16 channels of LBR-G.711 transcoding

Figure 21-5 shows a physical representation of the Catalyst 4000 voice gateway module in gateway mode.

Figure 21-5 Catalyst Voice Gateway Module in Gateway Mode



Gateway mode designates the default configuration. You can change the conferencing-to-transcoding ratios from the CLI.

The following configuration notes apply to the 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 CallManager. For all PSTN gateway functions, the Catalyst 4000 module uses H.323v2 and is configured identically to a Cisco IOS Gateway. From the Cisco CallManager configuration window, add the Catalyst 4000 gateway as an H.323 gateway.
- 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 CallManager. Specify a loopback IP address for the local Signaling Connection Control Part (SCCP).
- You can define a primary, secondary, and tertiary Cisco CallManager for both the conferencing services and MTP transcoding services.

Catalyst 6000 Voice Services

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 Catalyst 6000. This module comprises eight channel-associated-signaling (CAS) or PRI interfaces, each of which has its own CPU and DSPs. Once the card has been added from Cisco CallManager as a voice gateway, you configure it as a conferencing or MTP transcoding node. 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, you would configure a transcoding node for each conferencing node.

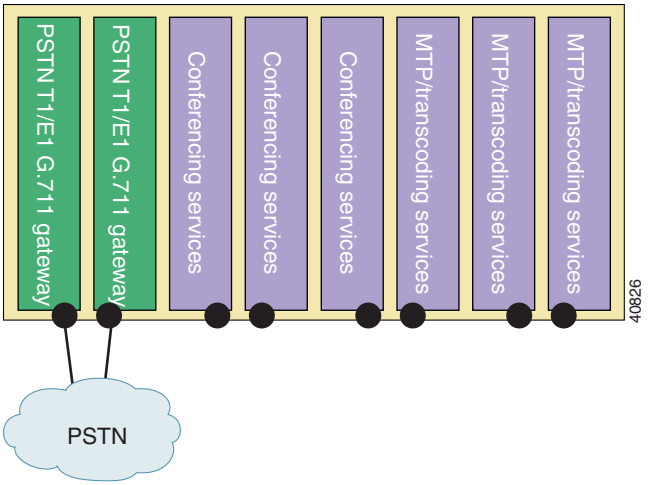
Whether acting as a PSTN gateway, a conferencing resource, or an MTP transcoding resource, each port on the module requires its own IP address. The port can be configured to have either a static IP address or an IP address provided by DHCP. If a static IP is entered, you must also add a TFTP server address

because the ports actually get all configuration information from the downloaded TFTP configuration file. Once configured through the Cisco CallManager interface, each *port* can support *one* of the following configurations:

- PSTN gateway mode: 24 sessions on the WS-6608-T1 module; 30 sessions on the WS-6608-E1
- Conferencing mode: 32 conferencing sessions for G.711 or G.723; 24 conferencing sessions for G.729
- MTP mode: 31 MTP transcoding sessions for G.723 to G.711; 24 MTP transcoding sessions for G.729 to G.711

Figure 21-6 shows one possible configuration of the Catalyst 6000 voice gateway module. This diagram shows two of the modules eight ports configured in PSTN gateway mode, three ports in conferencing mode, and three ports in MTP transcoding mode.

Figure 21-6 Catalyst 6000 Voice Gateway Module



Requirements and System Limits

The following sections describe the Catalyst DSP resources requirements and system limits for transcoding and conferencing.

MTP Transcoding Caveats

The following summary caveats apply to Catalyst MTP transcoding:

- Catalyst MTP transcoding service only supports LBR codec-to-G.711 conversion, and vice versa. No support exists for LBR-to-LBR codec conversion.
- On the Catalyst 6000, transcoding services cannot cross port boundaries.
- Make sure each Cisco CallManager has its own MTP transcoding resource configured.
- If transcoding is required between Cisco CallManager clusters, make sure the H.323 intercluster trunk is configured with an MTP resource. All calls between Cisco 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 heard.

See Table 21-1 for a list of transcoding capabilities for each module.

Conferencing Caveats

The following caveats apply to Catalyst conferencing services:

- The Catalyst 4000 conferencing services support G.711 connections only, unless an MTP transcoding service is used.
- On the Catalyst 6000, conferencing services cannot cross port boundaries.
- Each Cisco CallManager must have its own conferencing resource configured.

The section, "DSP Resource Manager" discusses conference calls across an IP WAN

Where to Find More Information

Related Topics

- Transcoders, page 18-1
- Conference Bridges, page 17-1

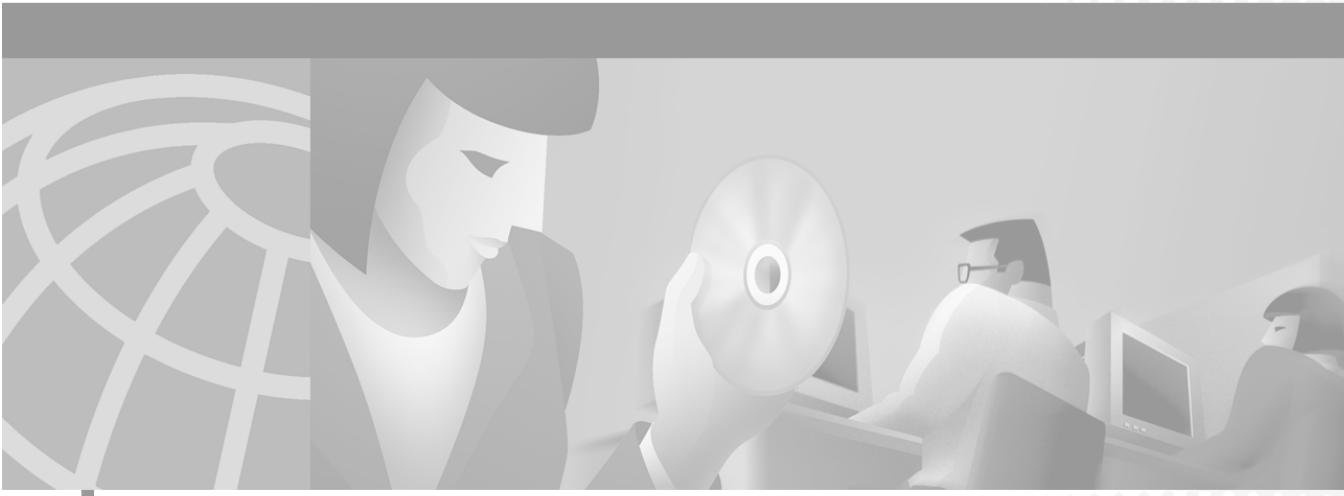
Additional Cisco Documentation

- *Cisco CallManager Administration Guide*
- *Cisco IP Phone 7900 Family Administration Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/7900/
- Cisco IP Phone user documentation and release notes (all models)

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

Cisco Systems



Part 6

Voice Mail and Messaging Integration

CHAPTER 22

SMDI Voice Mail Integration

Simplified Message Desk Interface (SMDI) defines a way for a phone system to provide voice-mail systems with the information needed to intelligently process incoming calls. Each time the phone system routes a call, it sends an EIA/TIA-232 message to the voice-mail system that tells it the line it is using, the type of call it is forwarding, and information about the source and destination of the call.

The SMDI-compliant voice-mail system connects to Cisco CallManager in two ways:

- Using a standard serial connection to the Cisco CallManager
- Using POTS line connections to a Cisco Access Analog Station gateway

This section covers the following topics:

SMDI Voice Mail Integration Requirements

The Cisco Messaging Interface service allows you to use an external voice-mail system with the Cisco CallManager 3.0 and later.

The voice-mail system must meet the following requirements:

- The voice-mail system must have a simplified message desk interface (SMDI) accessible with a null-modem EIA/TIA-232 cable (and an available serial port).
- The voice-mail system must use analog ports for connecting voice lines.

- The Cisco CallManager server must have an available serial port for the SMDI connection.
- A Cisco Access Analog Station Gateway, Cisco Catalyst 6000 24-port FXS Gateway, or Cisco VG200 Gateway must be installed and configured.
- Gateways are configured in a route pattern. See the "Route Pattern Configuration" chapter in the *Cisco CallManager Administration Guide* for more information.

Port Configuration for SMDI

Previous releases of Cisco CallManager required a specific configuration for voice-mail 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 reported by the Cisco Messaging Interface.

Beginning with Cisco CallManager Release 3.0(5), you can configure the SMDI port number through Cisco CallManager Administration.

Note You can still use the older style of configuration for FXS ports for voice mail, as long as the new SMDIPortNumber fields on the port configuration pane for analog access ports is not configured. If the SMDIPortNumber field is not configured, the default is 0. This default value applies for these fields for any upgrade of the current database configuration, and existing functionality is not affected.

To use the new SMDIPortNumber configuration, perform the following steps:

1. Modify each analog access port that connects to the voice-mail system and set the SMDIPortNumber equal to the actual port number on the voice-mail 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-mail system.

2. To take advantage of reduced Cisco CallManager signaling requirements with this new configuration, change each of the analog access devices that are in a route group 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 can be the same or different.

ReorderRouteList Service Parameter

An added mechanism allows selecting devices in a route group in a “round-robin” fashion. To take advantage of this feature, configure the devices as follows:

1. Configure all the analog access that connect to the voice-mail system in a single route group, with each device in the route group using “All Ports” and having the same selection order (that is, selection order 1).

2. Set the Cisco CallManager service parameter ReorderRouteList to T (True).

   When a call is extended via the route list, Cisco CallManager offers it to the devices in the route group in sequential order. Then, Cisco CallManager re-orders the device list (route group) by taking the first device in the list and moving it to the end of the list.

   The next call extended via the route list receives the re-ordered list, and thus extends the call to a different device (compared to the previous call). Each call attempt communicates with a subsequent device first. With this mechanism, use all devices in the group in a “round-robin” fashion instead of the current “top-down” only mechanism.

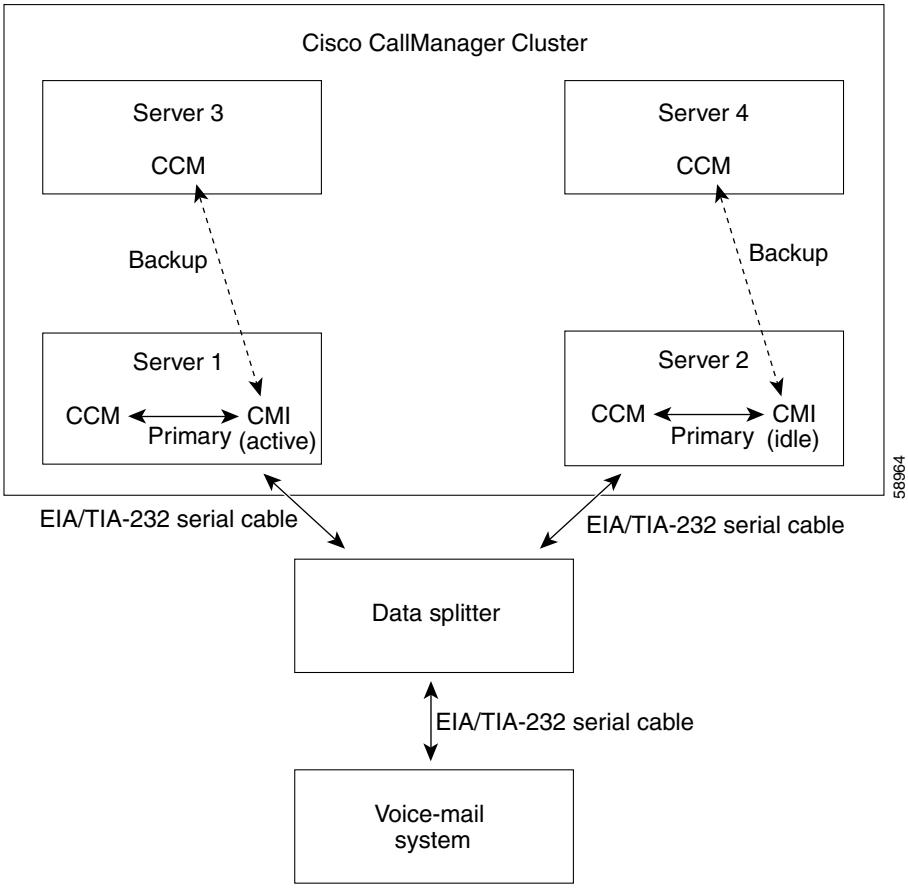
   Enabling the ReorderRouteList service parameter does not affect route list/route configurations that have explicitly set different selection orders for devices in a route group for setting up an ordered device selection (that is, the older method of voice-mail configuration).

CMI Redundancy

Most voice-mail systems relying 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 CMI redundancy by running two or more copies of the Cisco Messaging Interface service on different servers in a Cisco CallManager cluster and using additional hardware including a data splitter described later in this section.

Each copy of CMI connects to a primary and backup Cisco CallManager and registers to the Cisco CallManager using the same VoiceMailDn and VoiceMailPartition service parameter values. The CMI with the higher service priority (the active CMI service) handles the SMDI responsibilities. If this CMI encounters problems, another one can take over. Figure 22-1 illustrates one of many layouts that provides CMI redundancy.

Figure 22-1 CMI Redundancy



Note In order to achieve CMI redundancy, you must have a device such as the data splitter as shown in Figure 22-1 to isolate the SMDI messaging from the various CMI services. You cannot use an ordinary Y-shaped serial cable to combine the EIA/TIA-232 streams together.

The data splitter you connect to your voice-mail system, such as the B&B Electronics modem data splitter (models 232MDS and 9PMDS), must have the following characteristics:

- High reliability
- Bi-directional communication
- Minimal tranmission delay
- No external software support (desired)
- No extra RS-232 control line operations (desired)

The 232MDS has two DB25 male ports and one DB25 female port. The 9PMDS is a DB9 version of this modem data splitter. These switches enable CMI redundancy with the following limitations when you set the ValidateDNs CMI service parameter to *Off*:

- SMDI messages (MWI messages) from voice-mail systems are broadcast to both CMIs. Both CMIs send MWI messages to the Cisco CallManager to which they are connected. This produces an extra load on the database and network traffic (if the CMI and Cisco CallManager are on different servers.)
- Two CMIs cannot transmit SMDI messages simultaneously. Under extreme circumstances, you may experience network failures that break your Cisco CallManager cluster into two unconnected pieces. In the unlikely event that this occurs, both copies of CMI may become active, leading to the possibility that they may simultaneously transmit SMDI messages to the voice-mail system. If this happens, the collision could result in an erroneous message to the voice-mail system, which may cause a call to be mishandled.

SMDI Configuration Checklist

Table 22-1 provides an overview of the steps required to integrate voice-mail systems using SMDI:

Table 22-1 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 CallManager, *Cisco CallManager Administration Guide*
Step 2	Create a route group, and add the gateway ports you configured in Step 1 to the route group.	Adding a Route Group, *Cisco CallManager Administration Guide*
Step 3	Create a route list containing the route group configured in Step 2.	Adding a Route List, *Cisco CallManager Administration Guide*
Step 4	Create a route pattern.	Adding a Route Pattern, *Cisco CallManager Administration Guide*
Step 5	Install and configure the Cisco Messaging Interface service.	Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 6	Configure CMI trace parameters.	*Cisco CallManager Serviceability Administration Guide*
Step 7	Configure your voice-mail system, and connect the voice-mail system to Cisco CallManager with an EIA/TIA-232 cable.	Refer to the documentation provided with your system.

Where To Find More Information

Additional Cisco Documentation

- Cisco Messaging Interface Configuration, *Cisco CallManager Administration Guide*
- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco IP Telephony Network Design Guide*

CHAPTER 23

Cisco Unity Messaging Integration

Cisco Unity is a Windows NT and Windows 2000-based communications solution that delivers voice mail and unified messaging in a unified environment.

Unified messaging means that all types of messages can be managed from the same Inbox. Cisco Unity works in concert with an embedded Exchange server to collect and store all messages—including voice, fax, and e-mail—in one logical message store. Users can then access voice, fax, 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 CallManager with the Cisco Unity messaging system, refer to the *Cisco CallManager Integration Guide.*

This section covers the following topics:

System Requirements

The following lists provide requirements for your phone system and the Cisco Unity server:

Phone System

- Cisco CallManager software, version 3.0(9) or later, running on a Cisco IP telphony applications server.
- 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 CallManager extensions.
- A LAN connection in each location where you will plug an IP phone into the network.

Cisco Unity Server

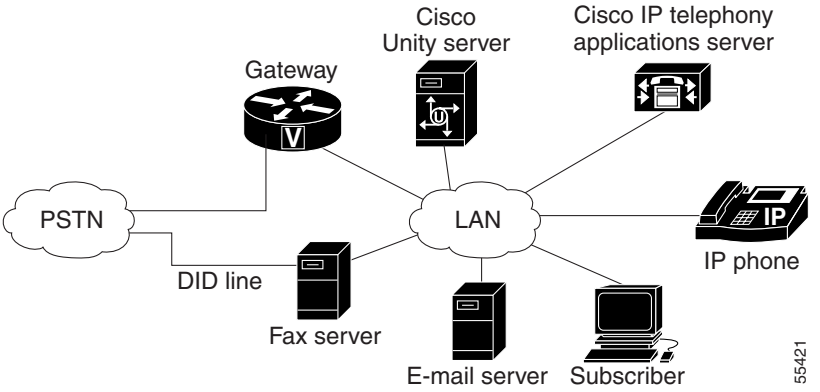
- Cisco Unity, Version 3.0(1) or later, installed and ready for the integration as described in the *Cisco Unity Installation Guid*e.
- A system key with the integration type set to “TAPI ” and with the appropriate number of voice-messaging ports enabled. If you are integrating Cisco Unity with two phone systems (Cisco CallManager and a second, non-IP phone system), you must set the integration type on the system key to “Multiple Integrations.”
- A Cisco license for each Cisco Unity port.

Integration Description

Figure 23-1 shows a full-featured Cisco Unity installation integrating with the Cisco Architecture for Voice, Video and Integrated Data (AVVID) network.

Note Some countries require a phone system between the public phone network and the gateway.

Figure 23-1 Connections Between the Phone System and Cisco Unity



The following steps give an overview of the path an external call takes through the Cisco AVVID network.

1. When an external call arrives, the Cisco gateway sends the call over the LAN to the machine on which Cisco CallManager is installed.
2. For Cisco CallManager lines that are configured to route calls to Cisco Unity, 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 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 CallManager Integration Guide* for more information.

Cisco Unity Configuration Checklist

Table 23-1 provides steps to configure the Cisco Unity voice-messaging system.

Table 23-1 Cisco Unity Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Ensure you have met the system requirements for Cisco CallManager and Cisco Unity.	See the "System Requirements" section on page 23-2. Refer to the *Cisco CallManager Integration Guide*.
Step 2	Add voice mail ports for each port that you are connecting to Cisco Unity.	Refer to the "Cisco Voice Mail Configuration" section in the *Cisco CallManager Administration Guide*. Refer to the *Cisco CallManager Integration Guide*.
Step 3	Specify MWI and voice mail extensions.	Refer to the "Service Parameters Configuration" section in the *Cisco CallManager Administration Guide*. Refer to the *Cisco CallManager Integration Guide*.
Step 4	Enable the DTMF relay feature in the gateways.	Refer to the gateway documentation for the model of gateway you are configuring. Refer to the *Cisco CallManager Integration Guide*.

Table 23-1 Cisco Unity Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 5	Install, configure, and test the TAPI service provider.	Refer to the *Cisco CallManager Integration Guide*.
Step 6	Configure Cisco Unity for the integration.	Refer to the *Cisco CallManager Integration Guide*
Step 7	Test the integration.	Refer to the *Cisco CallManager Integration Guide*. Refer to the installation guide for the phone system. Refer to the *Cisco Unity Troubleshooting Guide*.

Where to Find More Information

Additional Cisco Documentation

- Cisco Voice Mail Configuration, *Cisco CallManager Administration Guide*
- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- *Cisco CallManager Integration Guide*
- *Cisco Unity Installation Guide*
- *Cisco Unity Troubleshooting Guide*

CHAPTER 24

Cisco uOne Voice Messaging Integration

The optional Cisco Unified Open Network Exchange (uOne) software, available as part of Cisco IP Telephony Solutions, provides voice-messaging capability for users when they are unavailable to answer calls. This section provides an overview of the steps that must be performed within Cisco CallManager Administration to integrate Cisco CallManager with Cisco uOne Messaging.

To connect Cisco uOne to Cisco CallManager, you need to perform these tasks:

- Add Cisco uOne ports to Cisco CallManager. Enter all users and their directory numbers in Cisco CallManager Administration to retrieve messages from a Cisco uOne voice-mail device.
- Configure a message waiting indicator (MWI) device.
- Configure values for Cisco CallManager service parameters associated with Cisco uOne.
- Set Forward Busy and Forward No Answer for Cisco IP phones that will be accessing voice mail.

This section covers the following topics:

Cisco CallManager Service Parameters for Cisco uOne

You must set up the following Cisco CallManager service parameters when configuring Cisco CallManager to work with Cisco uOne:

- MessageWaitingOnDN and MessageWaitingOffDN—Cisco uOne uses the MWI On and MWI Off directory numbers specified by these two service parameters to turn the message waiting indicator (MWI) on a user phone on or off. The values for these parameters should match the CMMWIOffNumber value and the CMMWIOnNumber value in the Cisco uOne SSMWI.ini file. For more information about Cisco uOne .ini files, refer to the installation and configuration documentation supplied with Cisco uOne.

Note For Cisco IP Phone model 12 SP+ and 30 VIP, the phone button template for the user phone must have a button configured for Message Waiting for this feature to be available.

- VoiceMail—Voice-mail pilot number (the number users dial to call in to the voice-mail system). You must set this value for each Cisco CallManager in a cluster. Setting this parameter enables you to configure a single button on users phones for automatically dialing the voice-mail pilot number (for example, the messages button on a Cisco IP Phone 79xx). Make sure this number is the same as the Cisco uOne voice-mail pilot directory number configured in the Cisco uOne DialMap.ini file. Once you configure the VoiceMail parameter, you must stop and start Cisco CallManager or reset each phone.
- ForwardNoAnswerTimeout—Specifies the seconds to wait before forwarding on a No Answer condition. The recommended value is 12.
- ForwardMaximumHopCount—Specifies the maximum number of attempts to extend a forwarded call. The recommended value is 15.

Use the following procedure to configure the MWI On/Off directory numbers.

Before changing the values of the MWI On/Off service parameters, you must first stop the Cisco uLite process in Cisco uOne. Refer to the installation and configuration documentation shipped with Cisco uOne for more information.

Note You must set the MWI On/Off service parameters for each Cisco CallManager in the cluster.

Cisco uOne Configuration Checklist

Table 24-1 provides an overview of the steps required to integrate Cisco CallManager with Cisco uOne voice messaging:

Table 24-1 Cisco uOne Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Make sure the voice-mail pilot number and subsequent numbers are available. The Cisco uOne wizard requires a range of consecutive directory numbers for the Cisco uOne ports. The voice-mail pilot number to accesses the Cisco uOne server. The voice-mail pilot number specifies the number people call to access the Cisco uOne server. This number designates the Cisco voice-mail pilot directory number configured in the Cisco uOne DialMap.ini file.	Installation and configuration documentation supplied with Cisco uOne.
Step 2	Add a Cisco uOne server and ports to the Cisco CallManager database.	Cisco Voice Mail Configuration, *Cisco CallManager Administration Guide*
Step 3	Configure CallManager service parameter values.	Cisco CallManager Service Parameters for Cisco uOne Installation and configuration documentation supplied with Cisco uOne.

Table 24-1 Cisco uOne Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 4	Configure the MWI device.	Setting up the MWI Device, *Cisco CallManager Administration Guide* Installation and configuration documentation supplied with Cisco uOne.
Step 5	Set up Call Forward No Answer and Call Forward Busy on all Cisco IP phones that will be used with Cisco uOne.	Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*

Where to Find More Information

Additional Cisco Documentation

- Cisco Voice Mail Configuration, *Cisco CallManager Administration Guide*
- Service Parameters Configuration, *Cisco CallManager Administration Guide*

CHAPTER 25

Cisco DPA Integration

The Cisco DPA 7630 and 7610 Voice Mail Gateways (DPA 7630/7610) let you integrate Cisco CallManager systems with Octel voice mail systems, which might also be connected to either Lucent Definity G3 (Definity) or Meridian 1 (Meridian 1) PBX systems. The DPA 7630/7610 lets you 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 IP phones (connected to Cisco 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 3.0(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)
- Lucent Definity G3 PBX systems (DPA 7630 only)
- Nortel 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

The DPA 7630/7610 functions as a gateway between Cisco CallManager and an Octel system (which may be connected to a PBX system), performing these tasks:

- Determines the call type from Cisco 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 CallManager.
- Converts dual-tone multi-frequency (DTMF) tones to Skinny Client Control Protocol (SCCP) messages.
- Provides companding-law transcoding, and voice compression.
- Performs Real-Time Transport Protocol (RTP) encapsulation of the voice message.

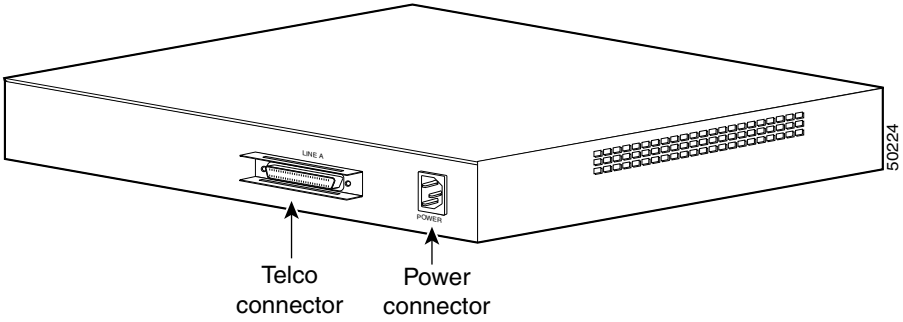
How the DPA 7630/7610 Works

With the Cisco DPA 7630/7610, you can integrate your existing Octel voice mail with Cisco 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 CallManager, Octel, Definity, and Meridian 1 systems.

Figure 25-1 illustrates the Cisco DPA.

Figure 25-1 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 CallManager, you must decide whether to do a complete cutover to Cisco CallManager or to migrate slowly. If you do a complete cutover to Cisco 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 installing new phones on the Cisco CallManager system. You might want to use your existing Octel voice-mail system with your Cisco CallManager system. In these cases, the DPA 7630/7610 can assist your migration to Cisco CallManager.

Can I Just Use SMDI?

Migration presents one difficulty because voice-mail systems such as Octel were designed to integrate to only one PBX at a time. To resolve this difficulty, you can use Simple Message Desk Interface (SMDI), which was designed to enable integrated voice-mail services to multiple clients.

However, to use SMDI, your voice mail system must meet several qualifications:

- It must have sufficient database capacity to support two PBX systems simultaneously and to associate each mailbox with the correct PBX in order 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 exists primarily 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, appearing 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 CallManager system.

However, the DPA 7630/7610 can translate these interfaces to enable communication among the Cisco CallManager, Octel, and Definity or Meridian 1 systems. Depending on the needs of your network, you can choose among several different integration methods.

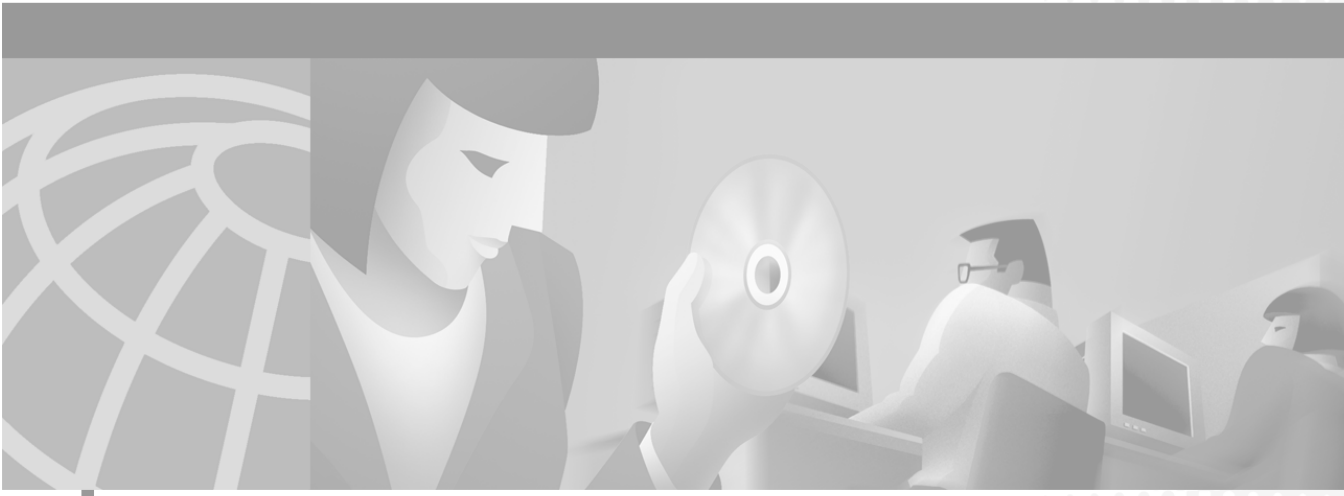
Where to Find More Information

Related Topics

- SMDI Voice Mail Integration, page 22-1

Additional Cisco Documentation

- *Cisco DPA 7630/7610 Voice Mail Gateways Administration Guide*



PART 7

System Features

CHAPTER 26

Call Park

The Call Park feature allows you to place a call on hold, so that 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 such as 1234. Someone on another phone in your system can then dial 1234 to retrieve the call.

The Call Park feature works within a Cisco CallManager cluster as well as between clusters. Each Cisco CallManager in a cluster can have call park extension numbers.

You can define either a single directory number or a range of directory numbers for use as call park extension numbers. Valid call park extension numbers consist of integers and characters. You can park only one call at each call park extension number.

This section covers the following topics:

Call Park Configuration Checklist

Table 26-1 provides a checklist to configure call park.

Table 26-1 Call Park Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure a call park number or define a range of call park extension numbers.	Adding a Call Park Number, *Cisco CallManager Administration Guide*
Step 2	Configure a partition for call park extension numbers to make it available only to users who have the partition in their calling search space.	Adding a Partition, *Cisco CallManager Administration Guide* and Media Termination Point Configuration, *Cisco CallManager Administration Guide*
Step 3	Configure park extension numbers on a per-Cisco CallManager basis.	Cisco CallManager Group Configuration, *Cisco CallManager Administration Guide*
Step 4	Notify users that the call park feature is available.	The *Cisco IP Phone 7960/7940 Getting Started Guide* contains instructions on how users access call park features on their Cisco IP Phone.

Where to Find More Information

Related Topics

- Phone Button Template Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Partition Configuration, *Cisco CallManager Administration Guide*

- Call Park Configuration, *Cisco CallManager Administration Guide*
- Media Termination Point Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Phone 7900 Family Administration Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/7900/
- Cisco IP Phone user documentation and release notes (all models)

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

CHAPTER 27

Call Pickup and Group Call Pickup

Two features, call pickup and group call pickup, allow users to answer calls that come in on a directory number other than their own. The differences between call pickup and group call pickup are explained in "Understanding Call Pickup and Group Call Pickup."

This section covers the following topics:

Understanding Call Pickup and Group Call Pickup

Cisco IP phones provide two types of call pickup:

- Call pickup—allows users to pick up incoming calls within their own group. Cisco CallManager automatically dials the appropriate call pickup group number when a user activates this feature from a Cisco IP phone.
- Group call pickup—allows users to pick up incoming calls within their own group or in other groups. Users must dial the appropriate call pickup group number when activating this feature from a Cisco IP phone.

The same procedures apply for configuring both of these features. Group call pickup numbers apply to lines or directory numbers.

Using Call Pickup Features with Partitions to Restrict Access

You can restrict access to call pickup groups by assigning a partition to the call pickup group number. When this configuration is used, only the phones that have a calling search space that includes the partition with the call pickup group number can participate in that call pickup group. Make sure the combination of partition and group number is unique throughout the system.

- If call pickup group numbers are assigned to a partition, only those phones that can dial numbers in that partition can use the call pickup group.
- If partitions represent tenants in a multitenant configuration, make sure the pickup groups are assigned to the appropriate partition for each tenant.

A multitenant configuration provides an example of using partitions with call pickup groups. The pickup groups will be assigned to the appropriate partition for each tenant, and the group number would not be visible to other tenants.

Call Pickup Guidelines and Tips

The following guidelines and tips apply to using Call Pickup and group Call Pickup features:

- You do not need to reset phones to reflect changes related to call pickup groups, but you must update the database.
- Although different lines on a phone can be assigned to different call pickup groups, that would be confusing to users and is not recommended.

Call Pickup Configuration Checklist

Table 27-1 provides a checklist to configure call pickup.

Table 27-1 Call Pickup Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure partitions if you will be using them with call pickup or group call pickup numbers.	Adding a Partition, *Cisco CallManager Administration Guide* Using Call Pickup Features with Partitions to Restrict Access, page 27-2
Step 2	Configure a call pickup group number. The number must be a unique integer.	Adding a Call Pickup Group Number, *Cisco CallManager Administration Guide*
Step 3	Assign the call pickup group number you created in Step 2 to the directory numbers associated with phones on which you wish to enable call pickup: • Only directory numbers assigned to a call pickup group can use the Call Pickup feature. • If partitions are used with call pickup numbers, make sure that the directory numbers assigned to the call pickup number have a calling search space that includes the appropriate partitions.	Assigning Directory Numbers to a Call Pickup Group, *Cisco CallManager Administration Guide*
Step 4	Add a Call Pickup or Group Call Pickup button to the phone templates, if needed. You only need to do this for older Cisco IP Phone 12 SP, 12 SP+, and 30 VIP phones.	Modifying Phone Button Templates, *Cisco CallManager Administration Guide*
Step 5	Notify users that the call pickup feature is available.	The *Cisco IP Phone 7960/7940 Getting Started Guide* contains instructions on how users access call pickup features on their Cisco IP Phone.

Updating Call Pickup Configurations

The following notes apply to updating call pickup configurations:

- When you delete a call pickup group number, you disable the call pickup feature for all directory numbers assigned to that group. To enable call pickup again for those directory numbers, you must reassign each of them to a new call pickup group.
- When you update a call pickup group number, Cisco CallManager automatically updates all directory numbers assigned to that call pickup group.
- You do not need to reset phones to reflect changes related to call pickup groups, but you must update the database.

Where to Find More Information

Related Topics

- Phone Button Template Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Partition Configuration, *Cisco CallManager Administration Guide*
- Call Park Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Phone 7900 Family Administration Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/7900/
- Cisco IP Phone user documentation and release notes (all models)

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

CHAPTER 28

Cisco IP Phone Services

System Administrators use the Cisco IP Phone Services Configuration area of Cisco CallManager Administration to define and maintain the list of Cisco IP phone services to which users can subscribe at their site. Cisco IP phone services include XML applications that enable the display of interactive content with text and graphics on Cisco IP phones.

Note Currently, only Cisco IP Phone 7960 and 7940 model phones support Cisco IP phone services.

Once the list of services is configured, users can log on to the Cisco CallManager user preferences pages and subscribe to these services for their Cisco IP phones or an administrator can add services to Cisco IP phones and device profiles.

Cisco CallManager [Release 3.0(5) or later] provides sample Cisco IP phone services applications. You can also create customized Cisco IP phone applications for your site.

This section covers the following topics:

Understanding Cisco IP Phone Services

Cisco IP Phone Services comprise XML applications that enable the display of interactive content with text and graphics on Cisco IP phones.

The Cisco IP Phone 7960 and 7940 model telephones have a button labeled "services." When the user presses this 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 their phone. The user then chooses a service from the listing. When a service is chosen from the menu, the URL is requested via HTTP, and a server provides the content, which then updates the phone display.

Typical services that might be supplied to a phone include weather information, stock quotes, and news quotes. Deployment of Cisco IP Phone Services occurs using the HTTP protocol from standard web servers, such as the Microsoft Internet Information Service (IIS).

Users can only subscribe to services configured through Cisco CallManager Administration. The following list gives information 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.

You can subscribe a lobby phone or other shared devices to a service from the Cisco CallManager Administration.

After the system administrator configures the services, users can log on to the Cisco IP Phone Configuration pane and subscribe to services. From the Cisco IP Phone Configuration pane, users can

- Customize the name of the service as it displays on their services list
- Enter any service parameters available for the chosen phone service
- Review the description of each phone service parameter
- Subscribe to that service on their phone (Subscriptions are made on a per-device basis.)

You can also subscribe to services from the Cisco CallManager Administration and from the Bulk Administration Tool (BAT) application.

When the user clicks the Subscribe button, Cisco 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 IP phone displays graphics or text menus, depending on how the services are configured.

The Cisco IP Phone 7960 model supports the HTTP header sent with any page that includes a Refresh setting. Therefore, a new page can replace any XML object displayed after a fixed time. The user can force a reload by quickly pressing the Update soft key. If a timer parameter of zero was sent in the header, the page only moves to the next page when the Update soft key is pressed. The page never automatically reloads.

The Cisco IP Phone 7960 model supports the following soft keys intended to help the data entry process:

- Submit—This indicates that the form is complete and the resulting URL should be sent via HTTP.
- <<—Backspace within a field.
- Cancel—Cancels the current input.

Use the vertical scroll button for field-to-field navigation.

Caution Do not put Cisco IP Phone Services on any Cisco CallManager server at your site or any server associated with Cisco CallManager, such as the TFTP server or directory database publisher server. This precaution eliminates the possibility of errors in a Cisco IP Phone Service application having an impact on Cisco CallManager performance or interrupting call-processing services.

Cisco IP Phone Service Configuration Checklist

Table 28-1 provides a checklist to configure Cisco IP phone service.

Table 28-1 Cisco IP Phone Service Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure Cisco IP Phone Services to the system. Each service has a name and description, which helps users browsing the system.	Adding a Cisco IP Phone Service, *Cisco CallManager Administration Guide*
Step 2	Configure the list of parameters used to personalize a service for an individual user.	Adding a Cisco IP Phone Service Parameter, *Cisco CallManager Administration Guide*
Step 3	Notify users that the Cisco IP Phone Service feature is available.	The *Cisco IP Phone 7960/7940 Getting Started Guide* contains instructions on how users access call pickup features on their Cisco IP phone.

Where to Find More Information

Related Topics

- Phone Button Template Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Services Configuration, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Phone 7900 Family Administration Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/7900/
- Cisco IP Phone user documentation and release notes (all models)
  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

CHAPTER 29

Extension Mobility and Phone Login Features

Extension Mobility provides a method of organizing work spaces to significantly reduce the costs associated with permanent office accommodations. With extension mobility, instead of assigning offices, cubicles, and desks to individual employees, several different employees share office spaces on a rotational basis. This approach usually gets used in work environments in which employees do not routinely conduct business in the same place every day.

This section covers the following topics:

Understanding Extension Mobility and Phone Logins

The Extension Mobility feature allows users to configure any Cisco IP Phone 7940 or Cisco IP Phone 7940 IP phone as their own, on a temporary basis, by logging in to that phone. Once 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, her 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, his information appears. The Extension Mobility feature dynamically configures a phone according to the current user.

Note If a login device profile is configured for a Cisco IP Phone 7960 but the user logs into a Cisco IP Phone 7940, the phone takes on the attributes and capabilities of the Cisco IP Phone 7940. This is because there are fewer lines on a Cisco IP Phone 7940 than a Cisco IP Phone 7960. The Cisco IP Phone 7960 capabilities return when the user logs into a Cisco IP Phone 7960.

Previously, only administrators could change phone settings only through Cisco CallManager Administration. The Extension Mobility feature allows users to change phone settings themselves without accessing Cisco 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 provided in this release. Refer to the *Cisco CallManager Administration Guide* for more information.

Supported Phones and Features

This release provides Extension Mobility feature availability on Cisco IP phones that support Cisco IP phone XML services; currently, only the Cisco IP Phone 7940 and the Cisco IP Phone 7960 offer this feature.

Managing Device Profiles

A device profile comprises the set of attributes (services and/or features) associated with a particular device. Device profiles include name, description, phone template, add-on modules, directory numbers, subscribed services, and speed-dial information. Two kinds of device profiles exist: autogenerated and user. You can assign the user device profile to a user, so that, when the user logs

into a device, the user device profile you have assigned to that user loads onto that device as a default login device profile. Once a user device profile is loaded onto the phone, the phone picks up the attributes of that device profile.

You can also assign a user device profile to be the default logout device profile for a particular device. When a user logs out of a phone, for instance, the logout device profile loads onto the phone, giving that phone the attributes of the logout device profile. You can create, modify, or delete the user device profile in the Cisco CallManager Administration web pages.

Note On some phones, if a user device profile is used as the logout device profile, you cannot delete the user device profile.

The autogenerated device profile automatically generates when you update the phone settings and choose a current setting to generate an autogenerated device profile. The autogenerated device profile associates with a specific phone to be the logout device profile. You can modify the autogenerated device profile but not delete it or change the profile name.

Note You may assign a default user device profile to a user for extension mobility purposes. If no profile is specified at the time of the login, Cisco CallManager uses the default profile.

Enabling and Disabling User Logins

You can enable or disable user logins via Cisco CallManager Administration. The following sections describe how to do this system-wide, per user, and per device.

System-Wide

You can enable or disable user logins on a system-wide basis within Cisco CallManager Administration by performing the following steps:

Step 1 Choose **Service > Service Parameters**.

Step 2 Choose the server on which you want to enable or disable the user login from the Server drop-down list and click **Next**.

Step 3 Choose Cisco Extension Mobility from the Service list box on the left side of the pane.

Step 4 From the Login Service Enabled field, choose True to enable the user login service, or False to disable it.

Note You can also set maximum login time and multi-login behavior information on this pane.

Step 5 Click **Update**.

Tips Click the "i" button on the upper right side of the pane for complete definitions of each field.

Choosing True or False from this pane enables or disables user login capability throughout the entire system. Refer to *Cisco CallManager Administration Guide* for more detailed configuration information.

Per User

You can enable or disable user logins per user by either associating or disassociating a user with device profiles. You must associate users with a device profile in order for user to log in; therefore, you can disable user login by removing all device profiles from the user within the user pages of Cisco CallManager Administration. Refer to Adding a New User in the *Cisco CallManager Administration Guide* for more information.

Per Device

You can enable or disable user logins per device by checking or unchecking the Enable Extension Mobility Feature check box on the Phone Configuration pane in the Cisco CallManager Administration pages. Go to the Device menu and click **Add a New Device**. This takes you to the Phone Configuration pane. Refer to Cisco IP Phone Configuration in the *Cisco CallManager Administration Guide* for more information.

Login and Logout Applications Configuration

To configure the Login and Logout services, you must configure the Login and Logout applications through the Cisco IP Phone Services Configuration pane, accessible via the Cisco CallManager Administration menu as follows:

Choose **Feature > Cisco IP Phone Services**.

Refer to Cisco IP Phone Configuration in the *Cisco CallManager Administration Guide* for more information.

Users must then subscribe to the Login and Logout Service through their Cisco CallManager User web pages. Refer to Adding a New User in the *Cisco CallManager Administration Guide* for more information.

Note A user can change the login device profile settings from the Cisco CallManager Administration User panes; however, the change does not take affect until the user logs into the device.

Directory Configuration

Make sure the following information is supplied within and about the directory:

- The address/location of the LDAP server to query for user authentication.
- The URL of the Login service

Extension Mobility Configuration Checklist

Table 29-1 shows the logical steps for configuring the Extension Mobility feature in the Cisco CallManager.

Note Perform the following checklist with the assumption that the users and devices are already configured for standard, non-extension mobility use in the Cisco CallManager Administration database.

Table 29-1 Extension Mobility Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Create a new user for Cisco CallManager Extension Mobility.	*Cisco CallManager Extended Services Administrator's Guide* Adding a New User, *Cisco CallManager Administration Guide*
Step 2	Configure the Cisco Customer Response Application Engine for Cisco CallManager Extension Mobility. • Add the Login Application • Add the Logout Application • Add the Login Application http Trigger • Add the Logout Application http Trigger	*Cisco CallManager Extended Services Administrator's Guide*

Table 29-1 Extension Mobility Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 3	Configure Cisco CallManager for Extension Mobility. • Add the Cisco IP phone login service • Add the Cisco IP phone logout service • Set the service parameters • Create a default device profile for the phone • Create the default device profile for the user • Associate a user device profile to a user for Cisco CallManager Extension Mobility • Configure the Cisco IP phone for Cisco Extension Mobility (currently, only the Cisco IP Phone 7940 and Cisco IP Phone 7960)	*Cisco CallManager Extended Services Administrator's Guide* Cisco IP Phone Services Configuration, *Cisco CallManager Administration Guide* Service Parameters Configuration, *Cisco CallManager Administration Guide* Device Profile Configuration, *Cisco CallManager Administration Guide* Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
Step 4	Prepare the user for Cisco CallManager Extension Mobility	*Cisco CallManager Extended Services Administrator's Guide*

Tips You can enable Extension Mobility on an existing Cisco IP Phone 7940 and Cisco IP Phone 7960 either by using the Find and List search and choosing an existing phone or when adding a new phone.

Where to Find More Information

Related Topics

- Cisco IP Phone Services, page 28-1

Additional Cisco Documentation

- Device Profile Configuration, *Cisco CallManager Administration Guide*
- Adding a New User, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Services Configuration, *Cisco CallManager Administration Guide*
- *Cisco CallManager Extended Services Administrator's Guide*

CHAPTER 30

Understanding Cisco WebAttendant

Cisco WebAttendant, a plug-in application, allows you to set up Cisco IP phones as attendant consoles. Employing a graphical user interface, the Cisco WebAttendant client creates an attendant console that 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 Cisco WebAttendant to handle calls for a department or company, or another employee can use it to manage his own telephone calls.

The Cisco WebAttendant client installs on a PC with IP connectivity to the Cisco CallManager system. The client works with a Cisco IP phone that is registered to a Cisco CallManager system (one client for each phone that will be used as an attendant console). Multiple clients can connect to a single Cisco CallManager system.

The Cisco WebAttendant client application registers with and receives call dispatching services from the Cisco Telephony Call Dispatcher (TCD) services on the Cisco CallManager.

This chapter covers the following topics:

Requirements

See the following sections for PC client requirements and Cisco IP phone requirements for using Cisco WebAttendant:

Cisco WebAttendant Client Requirements

The following list provides Cisco WebAttendant PC client requirements:

- Operating system—Microsoft Windows 98, Windows 2000, or Windows NT 4.0 (Service Pack 3 or greater) workstation or server
- Microsoft Internet Explorer 5.0 or later web browser with Active X enabled

Caution If you use Microsoft Internet Explorer 4.0 or earlier, you must upgrade to Microsoft Internet Explorer 5.0 to use the Cisco WebAttendant client.

- Display adapter color palette setting—Minimum of 256 colors; select 16-bit color or greater for optimal display.
- Network connectivity to the Cisco CallManager

Cisco IP Phone Requirements for Use with Cisco WebAttendant

Cisco WebAttendant works in conjunction with a Cisco IP phone. The MAC address defined in the Settings dialog box of the Cisco WebAttendant application links the Cisco CallManager, Cisco WebAttendant client, and the Cisco IP phone.

Configure the Cisco WebAttendant client to connect the Cisco IP phone to its registered Cisco CallManager server. To do this, make sure the IP Address or Host Name field in the Cisco Telephony Call Dispatcher Settings section of the client Settings dialog box is the address of the Cisco CallManager server to which the Cisco IP phone is normally registered.

Cisco IP phones used with Cisco WebAttendant must meet the following guidelines:

- Use Cisco WebAttendant with any Cisco IP Phone 7960/7940 models, Cisco IP Phone 12-Series model, or Cisco IP Phone model 30 VIP.
- Make sure that the Cisco IP phone is added as a device in Cisco CallManager before it is used with Cisco WebAttendant.
- Do not use a shared-line appearance on any phone used with Cisco WebAttendant. Make sure directory numbers assigned to a Cisco IP phone do not appear on any other device in the system.
- Make sure the Cisco IP phone has buttons for Hold and Transfer.
- If using a headset, ensure the phone has a headset button (Cisco IP phone 7960/740 models) or an Answer/Release button assigned on the phone button template (older Cisco IP phone models).
- Configure a maximum of eight lines on Cisco WebAttendant or the phone button template for the Cisco IP Phone model 30 VIP. Configure a maximum of six lines for the Cisco IP Phone 7960.
- To ensure that a Cisco WebAttendant user can receive calls at any Cisco IP phone in the cluster, configure the same number of lines on every phone.
- Disable call waiting and call forwarding for lines and directory numbers on Cisco IP phones used as Cisco WebAttendant consoles.
- If a Cisco WebAttendant user will be logging in to Cisco WebAttendant at more than one phone, ensure that each phone is set up according to these guidelines and that each phone is registered with its own Cisco WebAttendant client.

Cisco WebAttendant Installation and Configuration

You access and install the Cisco WebAttendant client from the Cisco CallManager Application Plugin Installation pane. To locate the client plugin, open Cisco CallManager Administration and choose **Application > Install Plugins**.

Configure each Cisco WebAttendant client to meet the following criteria:

- Provide the Cisco WebAttendant user and password
- Connect to the correct Cisco CallManager TCD server and directory database
- Associate the MAC address of the Cisco IP phone you plan to use with the Cisco WebAttendant client

Understanding Cisco WebAttendant Users

Cisco WebAttendant users comprise special user accounts created in the Cisco WebAttendant User Configuration pane in Cisco CallManager Administration. Administrators can add or delete Cisco WebAttendant users and modify user IDs and password information from Cisco CallManager Administration.

Before a user can log in to a Cisco WebAttendant client to answer and direct calls, you must add the user as a Cisco WebAttendant user and assign a password.

Note Be aware that Cisco WebAttendant user IDs and passwords are *not* the same as Directory users and passwords entered in the User area of Cisco CallManager Administration.

If a user cannot log in to the Cisco WebAttendant client, make sure that Cisco CallManager and Cisco TCD are both running. Verify that the user has been added in the Cisco WebAttendant User Configuration area of Cisco CallManager Administration and that the correct user name and password are specified in the client Settings dialog box.

Understanding the Cisco Telephony Call Dispatcher

The Cisco WebAttendant client application registers with and receives call dispatching services from the Cisco Telephony Call Dispatcher (TCD). The Cisco TCD, a Cisco CallManager service, provides communication among Cisco CallManager servers, Cisco WebAttendant clients, and the Cisco IP phones used with Cisco WebAttendant clients.

Note If you use Cisco WebAttendant in a cluster environment, make sure all Cisco CallManagers within a cluster have the Cisco TCD service installed and running. Cisco WebAttendant redundancy requires this setup to work properly; however, not all Cisco TCDs are required to have a route point.

Cisco TCD handles Cisco WebAttendant client requests for the following items:

- Call control (placing calls, answering calls, redirecting calls, putting calls on and taking calls off hold, and disconnecting calls)
- Call dispatching from pilot point to the appropriate hunt group destination
- Line status (unknown, available, on-hook, or off-hook)
- User directory information (Cisco TCD stores and periodically updates directory information for fast lookup by the Cisco WebAttendant client.)

Note Cisco TCD only monitors the status of internal devices and phones. A Cisco WebAttendant user cannot see line state for a phone that is connected to a gateway.

Cisco TCD also provides the mechanism for automated recovery for Cisco WebAttendant if a Cisco CallManager fails. If a Cisco CallManager fails, the following events occur:

- Another Cisco TCD service running on a Cisco CallManager within the cluster takes over servicing of the route points associated with the failed Cisco CallManager.
- The Cisco WebAttendant clients attached to the failed Cisco TCD service attempt to locate and connect to the Cisco TCD service on the Cisco CallManager server where their associated Cisco IP phone registered after failover.
- When the Cisco CallManager comes back up, its Cisco TCD will resume servicing its route points and Cisco WebAttendant clients.

Note No automated recovery for a Cisco TCD failure exists. If Cisco TCD stops running, all Cisco WebAttendant clients connected to that Cisco TCD do not work. Restart Cisco TCD to correct the problem.

Understanding Cisco TCD Database Path Options

In the Cisco WebAttendant client Settings dialog box, the Cisco TCD Database Path field controls where the Cisco WebAttendant client looks for its directory information. You can choose the default setting or set up the client to point to an alternate database.

Using wausers as the Default Setting for Cisco TCD Database Path

When the default setting is chosen, the Cisco WebAttendant client uses the Cisco TCD default database associated with the Cisco IP phone. To ensure that this default setting works properly, the Cisco CallManager administrator must rename the folder, C:\Program Files\Cisco\Users, to “wausers” and set network security and share permissions so that all Cisco WebAttendant users have read-and-write access. Ensure this task is done on all Cisco CallManagers in the cluster.

Cisco CallManager automatically makes directory database information available to Cisco WebAttendant clients and begins to update the information every 3 hours with the latest changes. How long it takes to update the information depends on factors like the size of your database.

Specifying a Location for the Cisco TCD Database Path

As an alternative to the default setting, copy the file named C:\Program Files\Cisco\Users\UsersDB1.mdb or C:\Program Files\Cisco\UsersDB2.mdb on the Cisco CallManager server to a different location. (This could be a file in a different shared directory on the network or a file on the Cisco WebAttendant user PC.) You must then point the Cisco WebAttendant client to this file by entering the path to the file in the Cisco TCD Database Path field in the client Settings dialog box.

When you specify a location for the Cisco TCD database, this does not make any changes through Cisco CallManager automatically available to the Cisco WebAttendant client. You must manually copy a new version of the database file to the new location when you need to update Cisco WebAttendant client users with database changes.

If you manually specify a Cisco TCD Database Path in the Settings dialog for the client, the client will use that setting until you change it. If you change the Cisco TCD Database Path setting for a Cisco WebAttendant client, you must restart the client for the change to take effect.

Caution Contact the Cisco Technical Assistance Center when you know that directory information is available, but no user can log in to Cisco WebAttendant.

Related Topics

- Setting Up the wauser Shared Directory for Cisco WebAttendant, *Cisco CallManager Administration Guide*
- Configuring Cisco WebAttendant Client Settings, *Cisco CallManager Administration Guide*

Cisco TCD Service and Trace Parameters

The Cisco WebAttendant Server Configuration pane lists service parameters and enables you to configure trace parameters for the Cisco Telephony Call Dispatcher (TCD). The following service parameters apply specifically to Cisco TCD:

Caution Do not change any listed service parameter without permission of a Cisco Technical Assistance Center engineer. Doing so may cause system failure.

- CCN Line State Port—This designates the TCP/IP port number used by the line state server to register and receive line and device information. The default value is 3223.
- LSS Access Password—Used at registration, this default password authenticates the line state server.
- LSS Listen Port—This TCP port designates where Cisco WebAttendant clients register with Cisco TCD for line and device state information. The default value is 3221.
- TCDServ Listen Port—This TCP port designates where Cisco WebAttendant clients register with Cisco TCD for call control. The default value is 4321.

Related Topics

- "Services", *Cisco CallManager System Guide*
- *CiscoCallManager Serviceability Administration Guide*

Understanding Pilot Points and Hunt Groups

A pilot point, a virtual directory number that is never busy, alerts the Cisco Telephony Call Dispatcher (TCD) to receive and direct calls to hunt group members. A hunt group comprises a list of destinations that determine the call redirection order.

For Cisco TCD to function properly, make sure the pilot point number is unique throughout the system (it cannot be a shared line appearance). When configuring the pilot point, you must choose one of the following options from the Pilot Point Configuration pane in Cisco CallManager Administration:

- First Available Hunt Group Member—Cisco TCD goes through the members in the hunt group in order until it finds the first available destination for routing the call.
- Longest Idle Hunt Group Member—This feature arranges the members of a hunt group in order from longest to shortest idle time. Cisco TCD finds the member with the longest idle time, and if available, routes the call. If not, Cisco TCD continues to search through the group. This feature evenly distributes the incoming call load among the members of the hunt group.

If the voice-mail number is the longest idle member of the group, Cisco TCD will route the call to voice mail without checking the other members of the group first.

Note Cisco recommends that you configure your pilot points and hunt groups through Cisco CallManager Administration before you install Cisco WebAttendant.

When a call comes into a pilot point, Cisco TCD uses the hunt group list and the selected call routing method for that pilot point to determine the call destination. During hunt group configuration, you must specify whether a hunt group member serves as a directory number (device member) or as a Cisco WebAttendant user plus a line number (user member). If a directory number is specified, Cisco TCD only checks whether the line is available (not busy) before routing the call. If a user and line number are specified, Cisco TCD confirms the following details before routing the call:

- The user must be logged in to Cisco WebAttendant.
- The user must be online.
- The line must be available.

When you specify a user and line number, the user can log in to and receive calls on any Cisco IP phone in the cluster controlled by Cisco WebAttendant.

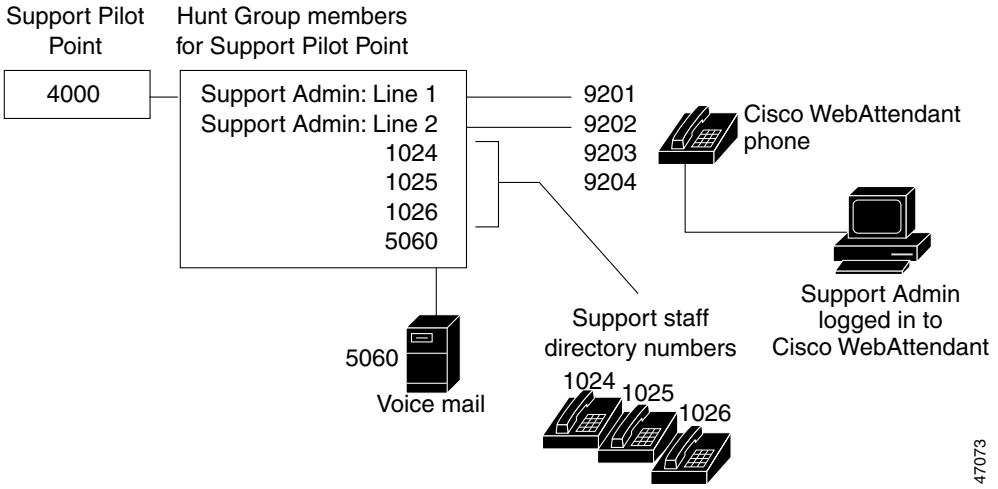
Caution To handle overflow conditions, configure your hunt groups so that Cisco TCD route calls to one or more Cisco WebAttendants or voice-mail numbers. To ensure that the voice-mail number can handle more than one call at a time, check the Always Route Member check box on the Hunt Group Configuration pane.

Example 30-1 Pilot Points and Hunt Groups Working Together

Assume a pilot point named Support exists at directory number 4000. The hunt group for the Support pilot point contains the following members:

- Support Admin, Line 1 and Support Admin, Line 2 (Support Admin is the Cisco WebAttendant login for the administrative assistant for Support.)
- Three directory numbers for support staff, 1024, 1025, and 1026, listed in the hunt group in that order
- A voice-mail number, 5060, which is the final member of the hunt group

Figure 30-1 Pilot Point and Hunt Group Example



As shown in Figure 30-1, the following example describes a simple call routing scenario where the user chose First Available Hunt Member during the configuration of the pilot point:

1. Cisco WebAttendant receives a call and directs it to the Support Pilot Point, directory number 4000.
2. Because 4000 is a pilot point and First Available Hunt Group Member is chosen as the call-routing option, the Cisco Telephony Call Dispatcher (TCD) associated with that pilot point checks the members of the hunt group in order, beginning with Support Admin, Line 1. Cisco TCD determines that the Support Admin user is not online, directory number 1024 is busy, directory number 1025 is busy, and directory number 1026 is available.
3. Cisco TCD routes the call to the first available directory number, which is 1026. Because 1026 is available, the Cisco TCD never checks the 5060 number.

Understanding Linked Hunt Groups

Linking hunt groups together allows the Cisco TCD to search through more than one hunt group when routing calls. When configured properly, pilot points create a link between hunt groups. Cisco TCD searches each hunt group according to the call-routing method chosen during configuration.

Consider the following guidelines when linking hunt groups together:

- Configure the individual pilot points and hunt groups first.
- For all except the last hunt group, make sure that the final member of the hunt group is the pilot point for the next hunt group. The pilot point from each group creates a link between the hunt groups, as seen inFigure 30-2.
- To handle overflow conditions, choose a voice-mail or auto-attendant number as the final member of the last linked hunt group in the chain. If Cisco TCD cannot route the call to any other members in the hunt groups, then the call goes immediately to the voice-mail number in the final hunt group.
- Check the Always Route Member check box on the Hunt Group Configuration pane only for the final member of each hunt group.

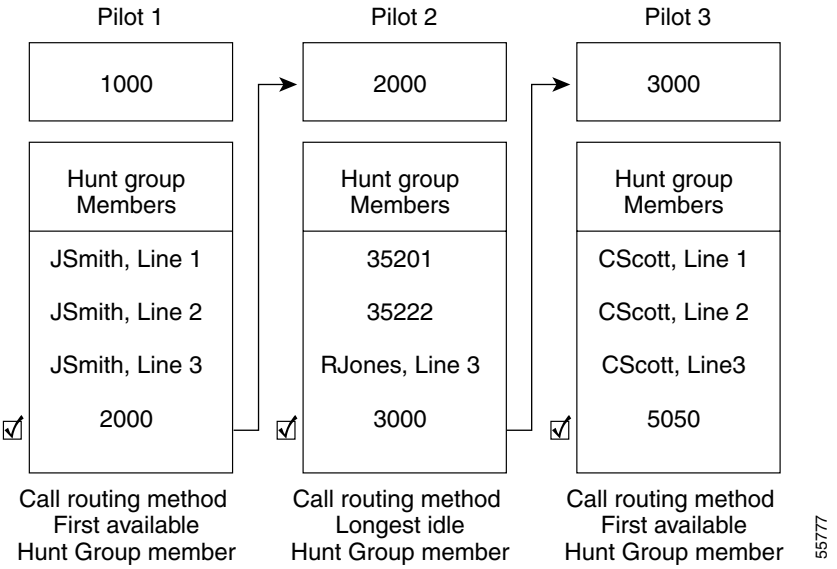
Caution Cisco strongly recommends that you do *not* link the last hunt group back to the first hunt group.

Example 30-2 Linked Hunt Groups Working Together

Consider the following information when referring to Figure 30-2:

- Three pilot points numbered 1, 2, and 3 exist at directory numbers 1000, 2000, and 3000, respectively.
- The last hunt group member of Pilot 1 acts as the pilot point for Pilot 2, while the last hunt group member of Pilot 2 serves as the pilot point for Pilot 3.
- During hunt group configuration, the administrator checked Always Route Member for the last member of each hunt group.
- Each hunt group contains four members, including the linked pilot point.
- JSmith, RJones, and CScott designate Cisco WebAttendant users specified as user/line pairs in the hunt groups.
- In Pilot 2, two directory numbers, 35201 and 35222, exist.
- The final hunt group member of Pilot 3, voice-mail number 5050, handles overflow conditions. The administrator checked Always Route Member when he configured this final hunt group member.

Figure 30-2 Linked Hunt Group Example



As represented in Figure 30-2, the following example describes a simple call-routing scenario for linked hunt groups:

1. Cisco WebAttendant receives a call and directs it to the first pilot point of the chain, directory number 1000.
2. Because 1000 is a pilot point and First Available Hunt Group Member is chosen as the call-routing method, the Cisco Telephony Call Dispatcher (TCD) checks the members in the hunt group in order, beginning with JSmith, Line 1. Cisco TCD determines that the first three members of the hunt group are unavailable and, therefore, routes the call to directory number 2000, the link to Pilot 2.

3. When the call reaches Pilot 2, Cisco TCD attempts to route the call to the longest idle hunt group member. Directory numbers 35201 and 35222 are busy, and RJones, Line 3, is offline. Cisco TCD routes the call to the last member of the group, directory number 3000, the link to Pilot 3.
4. Cisco TCD searches through Pilot 3 to find the first available member who is not busy. Cisco TCD determines that CScott, Line 2, is the first available member. Cisco TCD routes the call to that line. Cisco TCD never checks voice-mail number 5050.

Viewing Cisco WebAttendant Performance Monitors

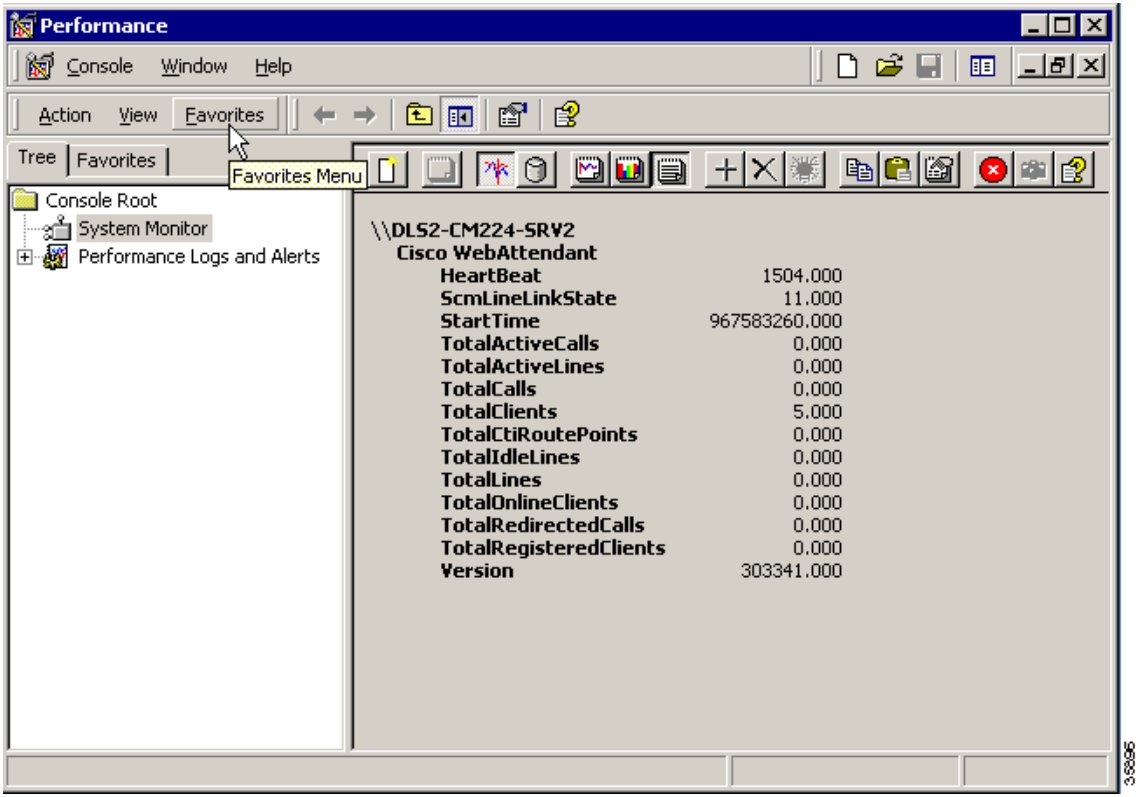
The CcmLineLinkState performance monitor for Cisco WebAttendant provides a quick way to check whether Cisco WebAttendant is functioning correctly:

- If the CcmLineLinkState counter is 11, Cisco TCD is functioning normally.
- The left-most digit of CcmLineLinkState indicates whether Cisco TCD is connected to and registered with the Cisco CallManager CTI. If this digit is 0, a problem may exist with the CTI or the directory.
- The right-most digit of CcmLineLinkState indicates whether Cisco TCD can perceive line state information through Cisco CallManager. If this digit is 0, a problem probably exists with Cisco CallManager.

Note When a Cisco WebAttendant user cannot log in to Cisco WebAttendant and no line state information is available, view the CcmLineLinkState performance monitor to verify that all components of Cisco WebAttendant are functioning properly.

When viewing a counter report for Cisco WebAttendant, as seen in Figure 30-3, you may see similar performance monitoring information.

Figure 30-3 Sample Performance Counter Report for Cisco WebAttendant



The following list gives other performance monitoring information provided for Cisco WebAttendant:

- Heartbeat—Number of seconds Cisco TCD has been running
- StartTime—Platform-based start time for this Cisco TCD
- TotalActiveCalls—Total number of active calls for this Cisco TCD
- TotalActiveLines—Total number of active lines for this Cisco TCD
- TotalCalls—Total of all calls handled by this Cisco TCD
- TotalClients—Number of Cisco WebAttendant clients associated with this Cisco TCD

- TotalCtiRoutePoints—Number of pilot points (route points) for this Cisco TCD
- TotalOnlineClients—Number of Cisco WebAttendant clients currently logged in and online
- TotalRedirectedCalls—Total number of calls redirected by pilot points (route points) for this Cisco TCD
- TotalRegisteredClients—Number of Cisco WebAttendant clients registered with this Cisco TCD
- Version—Cisco TCD version

Cisco WebAttendant Configuration Checklist

Perform the following steps in the table to set up Cisco WebAttendant:

Table 30-1 Cisco WebAttendant Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Add Cisco WebAttendant users in Cisco CallManager Administration.	Adding a Cisco WebAttendant User, *Cisco CallManager Administration Guide*.
Step 2	Make sure that each Cisco WebAttendant user Cisco IP phone is set up correctly for use with Cisco WebAttendant.	Cisco IP Phone Requirements for Use with Cisco WebAttendant, page 30-2
Step 3	Set up pilot points and hunt groups in Cisco CallManager Administration.	Configuring Pilot Points, *Cisco CallManager Administration Guide* Configuring Hunt Groups, *Cisco CallManager Administration Guide*
Step 4	Make sure the Cisco Telephony Call Dispatcher service is running on all Cisco CallManagers in the cluster.	Starting the Cisco Telephony Call Dispatcher, *Cisco CallManager Administration Guide* Understanding the Cisco Telephony Call Dispatcher, page 30-5

Table 30-1 Cisco WebAttendant Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	On each Cisco CallManager in the cluster, create a wauser shared directory with read/write access for Cisco WebAttendant users. You must perform this step to ensure Cisco WebAttendant clients can display directory information.	Setting Up the wauser Shared Directory for Cisco WebAttendant, *Cisco CallManager Administration Guide* Understanding Cisco TCD Database Path Options, page 30-6 Viewing Cisco WebAttendant Performance Monitors, page 30-14
Step 6	Install and configure the Cisco WebAttendant client on each Cisco WebAttendant user PC.	Installing the Cisco WebAttendant Client, *Cisco CallManager Administration Guide* Configuring Cisco WebAttendant Client Settings, *Cisco CallManager Administration Guide* Cisco WebAttendant Client Requirements, page 30-2

Where to Find More Information

Related Topics

- Configuring Cisco WebAttendant Users, *Cisco CallManager Administration Guide*
- Related Topics, *Cisco CallManager Administration Guide*
- Configuring Hunt Groups, *Cisco CallManager Administration Guide*
- Installing the Cisco WebAttendant Client, *Cisco CallManager Administration Guide*
- Configuring Cisco WebAttendant Client Settings, *Cisco CallManager Administration Guide*
- Cisco WebAttendant Server Configuration, *Cisco CallManager Administration Guide*
- Setting Up the wauser Shared Directory for Cisco WebAttendant, *Cisco CallManager Administration Guide*

- Starting the Cisco Telephony Call Dispatcher, *Cisco CallManager Administration Guide*
- Viewing Cisco WebAttendant Performance Monitors, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability Administration Guide*

Custom Phone Rings

Cisco IP phones ship with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco CallManager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named RingList.xml) that describes the ring list options available at your site reside in the TFTP directory on each Cisco CallManager server.

This appendix describes how you can customize the phone ring types available at your site by creating your own PCM files and editing the RingList.xml file. This section covers the following topics:

Creating a Custom Phone Ring

The following procedure only applies to creating custom phone rings for the Cisco IP Phone 7940 and 7960 models.

Procedure

Step 1 Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines listed in the "PCM File Requirements for Custom Ring Types" section on page 31-3.

Step 2 Use an ASCII editor to edit the RingList.xml file. Refer to the "RingList.xml File Format" section on page 31-2 for information about how to format this file, along with a sample RingList.xml file.

Step 3 Save your modifications and close the RingList.xml file.

Step 4 Place the new PCM files you created in the C:\ Program Files\Cisco\TFTPPath directory on the Cisco TFTP server for each Cisco CallManager in your cluster.

RingList.xml File Format

The RingList.xml file defines an XML object that contains a list of phone ring types. Each ring type contains a pointer to the PCM file used for that ring type and the text that will display on the Ring Type menu on a Cisco IP phone for that ring. The C:\ Program Files\Cisco\TFTPPath directory of the Cisco TFTP server for each Cisco CallManager contains this file.

The `CiscoIPPhoneRingList` XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

The following characteristics apply to the definition names:

- `DisplayName` defines the name of the custom ring for the associated PCM file that will display on the Ring Type menu of the Cisco IP phone.
- `FileName` specifies the name of the PCM file for the custom ring to associate with `DisplayName`.
- The `DisplayName` and `FileName` fields must not exceed 25 characters.

The following sample shows a RingList.xml file that defines two phone ring types:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.raw</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.raw</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

`DisplayName` and `FileName` are required for each phone ring type. The RingList.xml file can include up to 50 ring types.

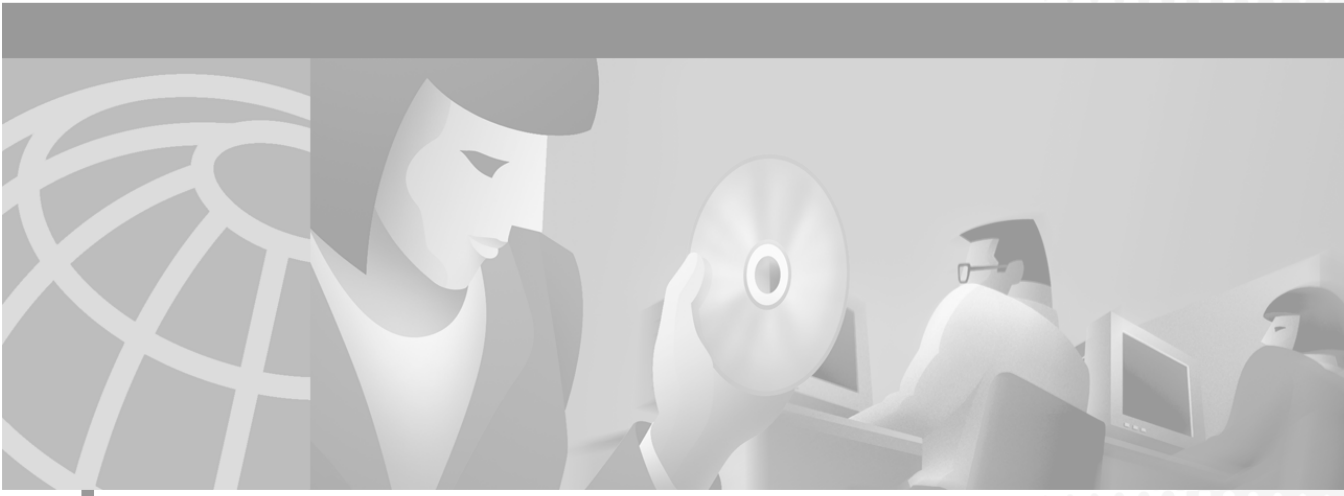
PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet the following requirements for proper playback on Cisco IP phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- uLaw compression
- Maximum ring size — 16080 samples
- Minimum ring size — 240 samples
- Number of samples in the ring is evenly divisible by 240.
- Ring starts and ends at the zero crossing.

You can use any standard audio editing packages that support these file format requirements to create PCM files for custom phone rings.

Cisco Systems



Part 8

Voice Gateways, Phones, and Computer Telephony Integration

CHAPTER 32

Understanding Voice Gateways

Cisco IP telephony gateways enable Cisco CallManager to communicate with non-IP telecommunications devices. Cisco CallManager supports several types of voice gateways.

This section covers the following topics:

Gateway Control Protocols and Trunk Interfaces

This section describes the gateway control protocols and trunk interface protocols that are supported for configuring gateways in Cisco CallManager.

- Gateway control protocols provide the internal interface between the voice gateway and Cisco CallManager.
- Trunk interfaces specify how the gateway interfaces with the PSTN or other external devices.

Gateway Control Protocols

Gateway control protocols provide communication and control between Cisco CallManager and the voice gateway.

The amount and type of information you configure in Cisco CallManager Administration versus what is configured on the gateway varies, depending on whether gateway control protocol is MGCP, H.323, or Skinny:

- **Media Gateway Control Protocol (MGCP)**—Gateways that support MGCP as of Cisco CallManager Release 3.1 include the Cisco VG200, Cisco 3600 and 2600, Cisco Catalyst 6000 8 Port Voice E1/T1 and Services modules, Cisco Catalyst 4000 Access Gateway Module, Cisco DE-30+, and Cisco DT-24+.

  When MGCP is used, the Cisco CallManager controls routing and tones and provides supplementary services to the gateway. MGCP provides call preservation (calls are maintained during failover and failback), redundancy, dial plan simplification (no dial peer configuration is required on the gateway), hookflash transfer, and tone on hold. MGCP-controlled gateways do not require an MTP to enable supplementary services such as hold, transfer, call pickup, and call park.

- **H.323**—The Cisco IOS integrated router gateways use H.323 protocol to communicate with Cisco CallManager. Intercluster trunks for connecting remote Cisco CallManagers across the IP WAN are also configured as H.323 gateways.

  Compared to MGCP, H.323 requires more configuration on the gateway, because the gateway must maintain the dial plan and route patterns.

- **Skinny Gateway Protocol**—Older Cisco voice gateways such as the AT-2, AT-4, AT-8, AS-2, AS-4, AS-8, and theCisco Catalyst 6000 24 Port FXS Analog Interface Module.

Trunk Interfaces

Device protocols specify the time-division multiplexing (TDM) signaling interface between the voice gateway and the PSTN or external non-IP telephony devices. Supported TDM interfaces vary by gateway model. The following list gives available interfaces:

- Foreign Exchange Office (FXO)—Use FXO ports for connecting to a central office or PBX. You can configure loop-start, ground-start, and E&M signaling interfaces, depending on the model selected.

Cisco CallManager assumes all loop start trunks lack positive disconnect supervision. We recommend that you configure trunks with positive disconnect supervision as ground start.

- Foreign Exchange Station (FXS)—Use FXS ports to connect to any Plain Old Telephone Service (POTS) device such as analog phones, fax machines, and legacy voice-mail systems.
- T1-PRI—Use this interface to designate North American ISDN Public Rate Interface with 23 bearer channels and one common channel signaling (CCS).
- E1-PRI—Use this interface to designate European ISDN Primary Rate Interface with 30 bearer channels, one CCS channel, and one framing channel.
- T1-CAS—Use this interface to designate T1 channel associated signaling (CAS), where each channel includes a dedicated signaling element. The supported signaling interface type is E&M.

Cisco Voice Gateways

Cisco CallManager supports several types of Cisco IP telephony gateways. These sections provide an overview of these supported gateways.

Standalone Voice Gateways

This section briefly describes the standalone, application-specific gateway models supported for use with Cisco CallManager.

Cisco Voice Gateway 200 Gateway

The Cisco IP Telephony 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 T1 PRI or T1-CAS ports for connecting to the PSTN
- 1 or 2 E1 PRI ports for connecting to the PSTN

- MGCP or H.323 interface to Cisco CallManager
  - MGCP mode supports T1/E1 PRI (user side only), T1-CAS, FXS, and FXO.
  - H.323 mode supports E1/T1 PRI (user side only), E1/T1-CAS, FXS, and FXO, and E&M, fax relay, G.711 modem.

The MGCP VG200 integration with legacy voice-mail systems allows the Cisco CallManager to associate a port with a voice mailbox and connection.

Cisco Access Digital Trunk Gateways DT-24+/DT30+

The Cisco Access Digital Gateways DT-24+/DE-30+ provide the following features:

- T1/E1 PRI (network or user side)
- T1-CAS connections (DT-24+) supporting E&M signaling with wink, immediate, or delay dial supervision; and loop start FXO and ground start circuit emulation.
- MGCP interface to Cisco CallManager

Cisco Analog Access Station Gateways

Station gateways let you connect the Cisco CallManager to POTS analog telephones, interactive voice response (IVR) systems, fax machines, and voice-mail systems. Station gateways provide FXS ports. The AS-2, AS-4, and AS-8 models accommodate two, four, and eight Voice over IP (VoIP) gateway channels, respectively.

Cisco AS gateways communicate with Cisco CallManager using SGCP.

Cisco Access Analog Trunk Gateways

Analog trunk gateways let you connect the Cisco CallManager to standard PSTN central office (CO) or PBX trunks. Trunk gateways provide FXO ports. The AT-2, AT-4, and AT-8 models accommodate two, four, and eight VoIP gateway channels. The signaling type is loop start.

Cisco AT gateways communicate with Cisco CallManager using SGCP.

Cisco Catalyst 4000 and 6000 Voice Gateway Modules

Several available telephony modules for the Cisco Catalyst 4000 and 6000 family switches act as telephony gateways enabling you to implement IP telephony in your network using existing Cisco Catalyst 4000 or 6000 family devices.

You can install Catalyst 6000 voice gateway modules that are line cards in any Cisco Catalyst 6000 or 6500 series switch. You can 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 feature as DT-24+/DE-30+)
  - DSP resources for transcoding and conferencing
- MGCP interface to Cisco CallManager

Depending upon which port type is configured, the ports can serve as T1/E1 interfaces, or the ports will support transcoding or conferencing.

Note Either blade supports DSP features on any port, but T1 blades cannot be configured for E1 ports, and E1 blades cannot be configured for T1 ports.

Users have the flexibility to use each port for T1/E1 connections or as network resources for voice services.

Cisco Catalyst 4000 Access Gateway Module

The Cisco Catalyst 4000 Access Gateway Module provides the following telephony features:

- 6 ports for FXS, FXO or E&M
- 2 T1/E1 ports for T1 PRI, T1-CAS, or E1 PRI
- MGCP interface to Cisco CallManager

Cisco Catalyst 4224 Access Gateway Module

The Cisco Catalyst 4224 Access Gateway Module provides the following features:

- 8 ports for FXS
- Supported protocols and interface types including
  - T1-PRI, E1-PRI, T1-CAS, E1-CAS R2, ISDN BRI, and FXO
- MGCP interface to Cisco CallManager

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 mail, IVR, POTS
- Cisco fax relay (T.38 Phase 2)
- MGCP interface to Cisco CallManager

The Catalyst 6000 24 Port FXS Analog Interface Module provides 24 FXS ports for connecting to analog phones, conference room speaker phones, and fax machines. You can also connect to legacy voice-mail systems. Using SMDI, you can associate the ports with voice-mail extensions.

The FXS module provides legacy analog devices with connectivity into the IP network, enabling them to utilize the IP network infrastructure for toll-bypass applications and to communicate with devices such as IP phones and H.323 end stations. This module also supports fax relay, which enables compressed fax transmission over the IP WAN, preserving valuable WAN bandwidth for other data applications.

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). You can also configure H.323 intercluster trunks to connect Cisco CallManagers in different clusters.

Cisco IOS H.323 Gateways

Cisco IOS H.323 gateways such as the Cisco 2600, 3600, 1750, 3810 V3, 7200 7500, AS5300, and VG200 provide full-featured routing capabilities as well as VoIP gateway functions. Refer to the documentation for each of these gateway types for information about support voice gateway features and configuration.

Intercluster Trunks

Use an intercluster trunk, an H.323 device, to connect two Cisco CallManagers in remote clusters. For information about configuring gatekeeper-controlled H.323 intercluster trunks for routing intercluster calls across a remote WAN link, refer to the *Cisco IP Telephony Network Design Guide*.

Voice Gateway Model Summary

Table 32-1 summarizes Cisco voice gateways supported by Cisco CallManager, with information about the gateway control protocols, trunk interfaces, and port types.

Table 32-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Ports

Gateway Model	Gateway Control Protocol	Trunk Interface	Port Types
Cisco IOS Integrated Routers			
Cisco 1750	H.323 (H.225)	FXS	POTS
		FXO	E&M
Cisco 3810 V3	H.323 (H.2250	T1-CAS	T1-CAS
		E1-CAS	E1-CAS
Cisco 2600	MGCP or H.323	FXS	POTS
		FXO	Loop start, ground start, E&M
		T1 PRI	T1 PRI
		T1-CAS	E&M
		E1 PRI	E1 PRI

Table 32-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Ports (continued)

Gateway Model	Gateway Control Protocol	Trunk Interface	Port Types
Cisco 3600	MGCP or H.323	FXS	POTS
		FXO	Loop start, ground start, or E&M
		T1 PRI	T1 PRI
		T1-CAS	E&M
		E1 PRI	E1 PRI
Cisco 7200	H.323 (H.225)	T1/E1 CAS	T1/E1 CAS
		T1/E1 PRI	T1/E1 PRI
Cisco 7500	H.323 (H.225)	T1/E1 CAS	T1/E1 CAS
		T1/E1 PRI	T1/E1 PRI
Cisco AS5300	H.323 (H.225)	T1/E1 CAS	T1/E1 CAS
		T1/E1 PRI	T1/E1 PRI
Intercluster Trunk	H.323	Intercluster Trunk	Not applicable
Cisco Standalone Voice Gateways			
Cisco Voice Gateway 200 (VG200)	MGCP or H.323	FXO	Loop start, ground start, E&M
		FXS	POTS
		T1-PRI	T1-PRI
		T1-CAS	E&M
		E1 PRI	E1 PRI
Cisco Access Digital Trunk Gateway DE-30+	MGCP	E1-PRI	E1 PRI
Cisco Access Digital Trunk Gateway DT-24+	MGCP	T1-PRI	T1-PRI
		T1-CAS	E&M, loop start, ground start

Table 32-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Ports (continued)

Gateway Model	Gateway Control Protocol	Trunk Interface	Port Types
Cisco Access Analog Trunk Gateway (AT-2, AT-4, AT-8)	SGCP	FXO	Loop start
Cisco Access Analog Station Gateway (AS-2, AS-4, AS-8)	SGCP	FXS	POTS
Cisco Catalyst Voice Gateway Modules			
Catalyst 4000 Access Gateway Module (WS-X4604-GWY)	MGCP or H.323	FXS FXO T1 CAS	POTS Loop start, ground start, E&M
Cisco Catalyst 6000 8 Port Voice T1 and Services Module (WS-X6608-T1)	MGCP	T1-PRI T1-CAS	T1-PRI E&M, loop start, ground start
Cisco Catalyst 6000 8 Port Voice E1 and Services Module (WS-X6608-E1)	MGCP	E1-PRI	E1-PRI
Cisco Catalyst 6000 24 Port FXS Analog Interface Module	MGCP	Foreign Exchange Station (FXS)	POTS

Gateways, Dial Plans, and Route Groups

Use dial plans to access or call out to the PSTN; route groups; and group specific gateways. Remote Cisco CallManagers across the IP WAN are configured as intercluster (H.323) gateways.

The different gateways used within the Cisco IP Telephony Solutions have dial plans configured in different places:

- Configure dial plan information for both skinny and MGCP gateways in the Cisco CallManager.
- Typically configure H.323-based Cisco IOS software gateways dial plan configuration in Cisco CallManager to access that gateway and configure dial peers in the gateway to pass that call out the gateway.

The route group points to one or more gateways and can select the gateways for call routing based on preference. The route group can direct all calls to the primary device and then use the secondary devices when the primary is unavailable. This serves effectively as a trunk group. 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. Route groups can perform digit manipulation that will override what was performed in the route pattern.

Configuration information associated with the gateway defines how the call is actually placed.

You can configure an H.323 gateway to be gatekeeper-controlled. This means that before a call is placed to an H.323 device it must successfully query the gatekeeper. Multiple clusters for inbound and outbound calls can share H.323 gateways, but MGCP and SGCP-based gateways are dedicated to a single Cisco CallManager cluster.

Gateway Failover and Failback

This section describes how Cisco voice gateways handle failover and failback.

MGCP Gateways

MGCP gateways receive a list of Cisco CallManagers according to the Cisco CallManager group, defined for the device pool assigned to the gateway. A Cisco CallManager group can contain one, two, or three Cisco CallManagers, listed in priority order, that the gateway uses there. If Cisco CallManager #1 goes down, then Cisco CallManager #2 is used. If #1 and #2 go down, then #3 is used.

Failback is the process of recovering a higher-priority Cisco CallManager when a gateway fails over to a secondary or tertiary Cisco CallManager. For Cisco MGCP gateways, higher priority Cisco CallManagers are periodically checked, statuses are taken and, when determined ready, marked as available again. The gateway then reverts to the highest available Cisco CallManager when all calls have gone

idle, or within 24 hours, whichever occurs first. A failback may be forced by the administrator either by stopping the lower priority Cisco CallManager (calls are preserved), or by restarting the gateway (calls are terminated).

IOS H.323 Gateways

Using several enhancements to the **dial-peer** and **voice class** commands in Cisco IOS Release 12.1(2)T, Cisco IOS gateways can now support redundant Cisco CallManagers. A new command, **h225 tcp timeout** *seconds*, that has been added specifies the time 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 CallManager, it tries a second Cisco CallManager defined in another **dial-peer** statement. The Cisco IOS gateway shifts to the **dial-peer** statement with next highest **preference** setting.

The following example shows the configuration for H.323 gateway failover:

```
interface Loopback0
    ip address 1.1.1.1 255.255.255.0
    voip-gateway voip bind srcaddr 1.1.1.1
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, we recommend 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 used in the setup might vary depending on protocol (RAS, H.225, H.245 or RTP).

SGCP Gateways

SGCP gateways are identical to MGCP gateways in terms of Cisco CallManager redundancy, failover and failback.

Gateway Configuration Checklist

Table 32-2 provides an overview of the steps required to configure gateways in Cisco CallManager, along with references to related procedures and topics.

Table 32-2 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 you are configuring.
Step 2	Gather the information you need to configure the gateway to operate with Cisco CallManager and to configure the trunk interface to the PSTN or external non-IP telephony device.	For Gateway Configuration Settings, refer to the *Cisco CallManager Administration Guide*. For Port Configuration Settings, refer to the *Cisco 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 you are configuring.
Step 4	Add and configure the gateway in Cisco CallManager Administration.	For Adding Gateways to Cisco CallManager, refer to the *Cisco CallManager Administration Guide*.
Step 5	Add and configure ports on the gateway.	For Port Configuration Settings, refer to the *Cisco CallManager Administration Guide*.
Step 6	For FXS ports, add directory numbers, if appropriate.	For Adding a Directory Number and Directory Number Configuration Settings, refer to *Cisco CallManager Administration Guide*.

Table 32-2 Gateway Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 7	Configure the dial plan for the gateway for routing calls out to the PSTN or other destinations. This can include setting up a route group, route list, and route pattern for the Gateway in Cisco CallManager or, for some gateways, configuring the dial plan on the gateway itself.	For Dial Plan Architecture and Configuration, refer to the *Cisco IP Telephony Network Design Guide.* See the "Dial Plan Architecture" section on page -5.
Step 8	Reset the gateway to apply the configuration settings.	For Resetting and Restarting Gateways, refer to the *Cisco CallManager Administration Guide*.

Tips To get to the default web pages for gateway devices, you can use the IP address of that gateway. Make your hyperlink url = http://www.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.

Where to Find More Information

Related Topics

- Adding Gateways to Cisco CallManager, *Cisco CallManager Administration Guide*
- Gateway Configuration Settings, *Cisco CallManager Administration Guide*
- Port Configuration Settings, *Cisco CallManager Administration Guide*
- Directory Number Configuration Settings, *Cisco CallManager Administration Guide*

Additional Cisco Documentation

- *Cisco IP Telephony Network Design Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network/
- Cisco Voice Gateway 200 (VG200) documentation on CCO
  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access/vg_200/

CHAPTER 33

Cisco IP Phones

Cisco IP Phones as full-featured telephones can plug directly into your IP network. H.323 clients and CTI ports are software-based devices that you configure similarly to the Cisco IP phones. The Cisco CallManager 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.

Once 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 IP Phones

Table 33-1 provides an overview of the features available on the following Cisco IP phones supported by Cisco CallManager:

- Cisco IP Phone 7900 family (models 7960, 7940, and 7910)
- Cisco IP Phone 7914 expansion module
- Cisco IP Conference Station 7935
- Cisco IP Phone model 30 VIP
- Cisco IP Phone 12 series

Table 33-1 Supported Cisco IP Phones and Features

Cisco IP Phone Model	Description
Cisco IP Phone 7960	The Cisco IP Phone model 7960, a full-featured, six-line business set, supports the following features: • An information (***i***) button • Six programmable line or speed-dial buttons • Four fixed buttons for accessing voice-mail messages and adjusting phone settings, services, and directories • Four soft keys for accessing additional call detail and functionality • A large LCD display that shows call detail and soft key functions • An internal, two-way, full duplex speakerphone and microphone mute
Cisco IP Phone 7940	The Cisco IP Phone model 7940, a two-line business set with features similar to the Cisco IP Phone model 7960, includes the following features: • An information (***i***) button • Two programmable buttons (You can configure these buttons as two lines or one line and one speed dial.) • Four on-screen mode buttons for accessing voice-mail messages and adjusting phone settings, services, and directories • Four soft keys for accessing additional call detail and functionality • A large LCD display that shows call detail and soft key functions • An internal two-way, full duplex speakerphone and microphone mute

Table 33-1 Supported Cisco IP Phones and Features (continued)

Cisco IP Phone Model	Description
Cisco IP Phone 7914 Expansion Module	Cisco IP Phone 7914 Expansion Module extends the functionality of the Cisco IP Phone 7960 by providing 14 additional line appearance buttons. You can configure these buttons as lines or speed dial. The Cisco IP Phone 7914 Expansion Module has a LCD to identify the function of the button and the line status. You can daisy chain two Cisco IP Phone 7914 Expansion Modules to provide 28 additional lines or speed-dial buttons.
Cisco IP Phone 7910	The Cisco IP Phone 7910, a single-line, basic feature phone 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 CallManager Available features include Call Park, Redial, Speed Dial, Call Pickup, Conference, Forward All, Group Call Pickup, 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 designed to be used for hands-free dialing

Table 33-1 Supported Cisco IP Phones and Features (continued)

Cisco IP Phone Model	Description
Cisco IP Conference Station 7935	The Cisco IP Conference Station 7935 voice instrument, a full-featured, IP-based, full-duplex hands-free conference station for use on desktops and offices and in small-to medium-sized conference rooms, includes the following features: • Three soft keys 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, and feature and line status • A digitally tuned speaker and three microphones, allowing conference participants to move around while speaking • Microphone mute

Table 33-1 Supported Cisco IP Phones and Features (continued)

Cisco IP Phone Model	Description
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 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 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

H.323 Clients and CTI Ports

Cisco CallManager Administration enables you to configure software-based devices such as H.323 clients and CTI ports. Software-based Cisco 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 and NetVision Symbol phones.

You configure H.323 clients and CTI ports through the Phone Configuration pane in the Cisco CallManager Administration like you do phones, but they often require fewer configuration settings.

For instructions on how to configure H.323 clients and CTI ports, refer to the "Cisco IP Phone Configuration" chapter in the *Cisco CallManager Administration Guide*.

Phone Button Templates

Cisco 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 default templates included with Cisco CallManager or to custom templates you created. 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 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 IP phones that use this template continue to use this template once it is renamed.

Make sure all phones have at least one line assigned. Normally, this is button 1. Phones can have additional lines assigned, depending on the Cisco IP phone model. Phones also generally have several features, such as speed dial and call forward, 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. You must reassign all Cisco IP phones using the template you want to delete to a different phone button template before you can delete the template.

Cisco CallManager does not directly control all features on Cisco IP phones through phone button templates. Refer to the *Cisco IP Phone 7900 Family Administration Guide* and the *Getting Started* publications for individual Cisco IP Phone 7900 Family models for detailed information.

Default Phone Button Templates

Although all Cisco IP phones support similar features, you implement these features differently on various models. For example, some models configure features such as Hold or Transfer using phone button templates; other models have fixed buttons or on-screen program keys for these features that are not configurable. Also, the maximum number of lines or speed dials supported differs for some phone models. These differences require different phone button templates for specific models.

Each Cisco 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 33-2 provides descriptions of the default phone button template for each Cisco IP phone model.

Table 33-2 Default Phone Button Templates Listed by Model

Cisco IP Phone Model	Default Phone Button Template Description
Cisco IP Phone 7960	The default Cisco IP Phone 7960 template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dial. Access other phone features, such as call park, call forward, redial, hold, resume, voice mail, conferencing, and so on using soft keys on the Cisco IP Phone 7960.
Cisco IP Phone 7940	The Cisco IP Phone 7940 comes with two preconfigured phone button templates provided: • 7940 (2-Line)—Uses button 1 and 2 for lines. • 7940 (1-Line)—Uses button 1 for line 1 and button 2 for speed dial. All Cisco IP Phone 7940 phones use one of these templates. Access phone features, such as call park, call forward, redial, hold, resume, voice mail, conferencing, and so on, using soft keys on the Cisco IP Phone 7940.
Cisco IP Phone 7914 Expansion Module	The default Cisco IP Phone 7914 Expansion Module template uses buttons 1 through 11 for speed dial and leaves buttons 12 through 14 undefined. Access phone features, such as call park, call forward, redial, hold, resume, voice mail, conferencing, and so on, using soft keys on the Cisco IP Phone 7960. Each Cisco IP Phone 7914 Expansion Module can use a different template.
Cisco IP Phone 7910	The default phone button template for the Cisco IP Phone 7910 (named Default 7910) 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 IP Phone 7910 has fixed buttons for Line, Hold, Transfer, and Settings.

Table 33-2 Default Phone Button Templates Listed by Model (continued)

Cisco IP Phone Model	Default Phone Button Template Description
Cisco IP Conference Station 7935	Because this phone only has a single line, Cisco does not provide a default phone button template.
Cisco IP Phone 30 SP+	The default Cisco IP Phone model 30 SP+ template uses buttons 1 through 4 for lines, button 5 for call park, button 6 for redial, buttons 8 through 13 and 22 through 25 for speed dial, button 14 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).
Cisco IP Phone 30 VIP	The default Cisco IP Phone model 30 VIP template uses buttons 1 through 4 for lines, button 5 for call park, button 6 for redial, buttons 8 through 13 and 22 through 25 for speed dial, button 14 for message waiting indicator, button 15 for call forward, and button 16 for conference.
Cisco IP Phone 12 Series	All Cisco IP Phone model 12 Series phones (12 S, 12 SP, 12 SP+) use the default Cisco IP Phone model 12 SP+ template. The default Cisco IP Phone model 12 SP+ template uses 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.

Guidelines for Customizing Phone Button Templates

Use the following guidelines when 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 to be used by employees in your company, make sure it includes the following features and that you describe them on the quick reference card you create for your users:
  - Cisco IP Phone 7960, 7940—Line (one or more)
  - Cisco IP Phone 7910—Forward all
  - 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
- Consider the nature of each feature to determine how to configure your phone button template. You might want multiple buttons assigned to speed dial and line; however, you usually require only one of the other features described in Table 33-3.

Table 33-3 Phone 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 the called party hears when the calling party is using a speakerphone. Users should press the AEC button on a Cisco IP Phone 30 SP+ when using speakerphone. Users do not need to press this button when speakerphone is not in use. This feature requires no configuration 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.

Table 33-3 Phone Feature Description (continued)

Feature	Description
Auto answer	If this feature is programmed on the template, activating this button causes the speakerphone to go off-hook automatically when an incoming call is received.
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 configured in the system for this button to work, and you should provide that number or range to your users, so they can dial into the number(s) to retrieve calls.
Call pickup	Call pickup allows users to pick up incoming calls within their own group. When a user activates this feature, the phone dials the appropriate call pickup group number automatically.
Conference	When users press this button, they initiate an ad hoc conference and then conference other participants in one at a time. Only the person initiating an ad hoc conference needs a conference button. You must make sure an ad hoc conference device is configured in Cisco CallManager Administration for this button to work.
Forward all	Users press this button to forward all calls to the designated directory number. Users can designate the forward all in the Cisco IP Phone Configuration panes, or you can designate a forward all number for each user in Cisco CallManager Administration.
Group call pickup	Group call pickup allows users to pick up incoming calls within their own group or in other groups. Users must dial the appropriate call pickup group number when using this feature.

Table 33-3 Phone 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 hears 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. You must have added directory numbers on the user phone for this button to work.
Meet-Me conference	When users press this button, they initiate a meet-me conference, and they expect other invited users to dial into the conference. Only the person initiating a meet-me conference needs a meet-me button. You must make sure a meet-me conference device is configured in Cisco 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 dialed on the Cisco IP phone. This feature requires no configuration to work.
Speed-dial	Users press this button to speed dial a specified number. System administrators can designate speed-dial numbers in Cisco CallManager Administration. Users can designate speed-dial numbers in the Cisco IP Phone Configuration panes.
Transfer	Users press this button to transfer an active call to another directory number.This feature requires no configuration to work.

Methods for Adding Phones

You can automatically add phones to the Cisco CallManager database using auto-registration, manually using the phone configuration panes, or in groups with the Bulk Administration Tool (BAT).

By enabling auto-registration before you begin installing phones, you can automatically add a Cisco IP phone to the Cisco CallManager database when you connect the phone to your IP telephony network. For information on enabling auto-registration, refer to the "Enabling Auto-Registration" section in the *Cisco CallManager Administration Guide*. During auto-registration, Cisco CallManager assigns the next available sequential directory number to the phone. In many cases, you might not want to use auto-registration; for example, if you want to assign a specific directory number to a phone.

If you do not use auto-registration, you must manually add phones to the Cisco CallManager database or use the Bulk Administration Tool (BAT). BAT, a plug-in application, enables system administrators to perform batch add, modify, and delete operations on large numbers of Cisco IP phones. Refer to the *Bulk Administration Tool Guide for Cisco CallManager* for detailed instructions on using BAT.

Directory Numbers

Using Cisco CallManager, you can configure and modify directory numbers (lines) assigned to specific phones.

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

In a shared line appearance, for example, you can set up a shared line so that 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 would be a single incoming 800 number that is set up to appear as line 2 on every sales representative phone in an office.

The following notes and tips apply to using shared line appearances with Cisco CallManager:

- You create a shared line appearance by assigning the same directory number and partition to different lines on different devices.
- If other devices share a line, the words Shared Line display in red next to the directory number in the Configure a Line Number pane in Cisco CallManager Administration.
- If you change the Calling Search Space, Call Waiting, 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 number for the line and update the device.
- In the case of a shared line appearance, Delete removes the directory number only on the current device. Other devices are not affected.
- Do not use shared line appearances on any phone that will be used with Cisco WebAttendant.
- Do not use shared line appearances on any Cisco IP Phone 7960 that requires auto-answer capability.

Phone Features

Cisco CallManager enables you to configure these phone features on Cisco IP phones: call waiting, call forward, call park, and call pickup.

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.

Configure call waiting on the Directory Number Configuration pane in Cisco CallManager Administration.

Call Forward

Call forward allows a user to configure a Cisco IP phone so that all calls destined for it ring another phone. Three types of call forward exist:

- Call forward all—Forwards all calls.
- Call forward busy—Forwards calls only when the line is in use.
- Call forward no answer—Forwards calls when the phone is not answered after the configured number of rings.

Configure call waiting on the Directory Number Configuration pane in Cisco CallManager Administration.

Call Park

Call park allows a user to place a call on hold, so that anyone connected to the Cisco 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. Anyone connected to the system can then dial 1234 to retrieve the call.

To use call park, you must add the call park extension (in this case, 1234) in Cisco CallManager Administration when configuring phone features. For more information about call park, see "Call Park" section on page 26-1.

Call Pickup

Call pickup allows you to use your phone to answer another ringing phone in your designated call pickup group.

You configure call pickup when configuring phone features in Cisco CallManager.

When adding a directory line, you can indicate the call pickup group. The call pick up 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, see "Call Pickup and Group Call Pickup" section on page 27-1.

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 "Associating Devices to a User" in the *Cisco CallManager Administration Guide*.

Phone Administration Tips

The following sections contain information that might help you configure phones in the Cisco CallManager Administration.

Phone Search

The following sections describe how to modify your search to locate a phone. If you have thousands of Cisco IP phones in your network, you might need to limit your search to find the phone you want. If you are unable to locate a phone, you may need to expand your search to include more phones.

Note The phone search is not case sensitive.

Searching by MAC Address

To search for a phone by its MAC address, choose **Device Name** and **ends with**, and enter the last 4 or 5 characters in the MAC address.

Searching by Description

If you enter a user name and/or extension in the Description field when adding the phone, you can search by that value on the Find and List Phones pane.

Searching by Calling Search Space or Device Pool

If you choose calling search space or device pool, the options available in the database display, you can choose one of these options from the drop-down list box below the Find button.

Finding All Phones in the Database

To find all phones registered in the database, choose Device Name from the list of fields; choose "is not empty" from the list of patterns; then, click **Find**.

Note The list on the Find and List Phones pane does not include analog phones and fax machines connected to gateways (such as a Cisco VG200). This list shows only phones configured in Cisco CallManager Administration.

Messages Button

You can configure a voice-mail access number for the messages button on Cisco IP Phone 7960/7940, so that users can access voice mail by simply pressing the messages button by performing the following actions:

1. Configure the Cisco CallManager VoiceMail service parameter with the voice-mail DN.
2. Repeat this procedure for all Cisco CallManagers in the cluster.
3. Reset the phones in the cluster for the change to take effect.

For information on how to access the Service Parameters Configuration pane, refer to the "Updating a Service Parameter" section in the *Cisco CallManager Administration Guide*.

Note For Cisco IP Phone model 12 SP+ and 30 VIP, you can access voice mail by configuring a button with the message waiting feature using a phone button template.

Directories Button

The Cisco IP Phone 7960/7940 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 configured with Cisco CallManager.

The URL Directories enterprise parameter defines the URL that points to the global directory for display on Cisco IP Phone 7960/7940 phones. The XML device configuration file for the phone stores this URL.

Tips

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.

To verify that the phone is accessing the correct URL after you change the URL directories enterprise parameter, perform the following steps on the Cisco IP phone: press **settings**, **3** (Network Configuration); then, press **27** (Directories URL).

If the phone URL was not updated correctly after changing the URL Directories parameter, try stopping and restarting the Cisco TFTP service; then, reset the phone.

MaxStationsInitPerSecond Service Parameter

The CallManager uses the MaxStationsInitPerSecond parameter to control the number of phones registered per second. The Cisco CallManager queues the registration messages up front and processes them at the rate you specify. The default specifies 10 phones per second. You can modify the MaxStationsInitPerSecond parameter on the Service Parameters Configuration pane. If the performance value is set too high, phone registrations could slow the Cisco CallManager real-time response. If set too low, the total time for a large group of phones to register will be slow.

Phone Failover and Failback

This section describes how phones failover and failback if the Cisco CallManager to which they are registered becomes unreachable. This section also covers conditions that can affect calls associated with a phone, such as reset or restart.

Cisco CallManager fails or becomes unreachable

The active Cisco CallManager is the Cisco CallManager from which the phone receives call processing services. The active Cisco CallManager usually serves as the primary Cisco CallManager for that phone (unless the primary is not available.)

If the active Cisco CallManager fails or becomes unreachable, the phone attempts to register with the next available Cisco CallManager in the Cisco CallManager Group specified for the device pool to which the phone belongs

The phone device reregisters with the primary Cisco CallManager as soon as it becomes available after a failure.

Phone is reset

If a call is in progress, the phone does not reset until the call is finished.

Phone Configuration Checklist

Table 33-4 provides steps to manually configure a phone in the Cisco CallManager Administration. If you are using auto-registration, Cisco CallManager adds the phone and assigns the directory number automatically.

Table 33-4 Phone Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Gather the following information about the phone: • Model • MAC address • Physical location of the phone • Cisco 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 33-17
Step 2	Add and configure the phone.	Adding a Phone, *Cisco CallManager Administration Guide*
Step 3	Add and configure lines (DNs) on the phone. You can also configure phone features such as call waiting, call forward, call park, and call pickup	Adding a Directory Number, *Cisco 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 assigned to them. Users can change the speed-dial buttons on their phones using the Cisco IP Phone Configuration panes.	Configuring Speed Dial Buttons, *Cisco CallManager Administration Guide*

Table 33-4 Phone Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 5	Configure Cisco IP phone services. You can configure services for Cisco IP Phone 7960/7940 models if you want to provide services for users or if you are configuring phones that do not have a specific user assigned to them. Users can change the services on their phones using the Cisco IP Phone Configuration panes.	Configuring Cisco IP Phone Services, *Cisco CallManager Administration Guide*
Step 6	Associate user with the phone (if required).	Associating Devices to a User, *Cisco CallManager Administration Guide*

Where to Find More Information

Related Topics

- Call Park, page 26-1
- Call Pickup and Group Call Pickup, page 27-1
- Enabling Auto-Registration, *Cisco CallManager Administration Guide*
- Configuring Cisco IP Phones, *Cisco CallManager Administration Guide*
- Associating Devices to a User, *Cisco CallManager Administration Guide*
- Updating a Service Parameter, *Cisco CallManager Administration Guide*

Additional Cisco CallManager Documentation

- *Cisco IP Phone 7900 Family Administration Guide*
- *Getting Started* publications for individual Cisco IP Phone 7900 Family models
- *Bulk Administration Tool Guide for Cisco CallManager*

CHAPTER 34

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 based on information provided by caller ID. CTI applications can also enable you to use information captured by an interactive voice response (IVR) system, so that the call can be routed to the appropriate customer service representative or so that the information is provided to the individual receiving the call.

This section covers the following topics:

Computer Telephony Integration Applications

The following list contains descriptions of some of the available Cisco CTI applications:

- Cisco IP SoftPhone—Cisco IP SoftPhone, 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 SoftPhone in tandem with a Cisco IP phone to place, receive and control calls from your desktop PC. All features function in both modes of operation.
- Cisco IP AutoAttendant—The Cisco IP AutoAttendant application works with Cisco CallManager to receive calls on specific telephone extensions and to allow the caller to select an appropriate extension.
- Cisco WebAttendant—Cisco WebAttendant provides a graphical user interface for controlling a Cisco IP phone to perform attendant console functions.
- Personal Assistant—Personal Assistant, a virtual secretary or personal assistant, can selectively handle your incoming calls and help you make outgoing calls.

Note When you create a user in Cisco CallManager Administration, and the user is going to use a CTI application, be sure to check the Enable CTI Application Use check box on the Add a User pane. If you do not check this check box, the CTI application does not work properly.

CTIManager

A program called CTIManager includes the CTI components that interface with the applications separated out of CallManager. The CTIManager service communicates with Cisco CallManager using the Cisco CallManager communication framework, System Distribution Layer (SDL). Installation of the CTIManager program occurs in the ..\Program Files\Cisco\bin\ folder on the Cisco CallManager server during the Cisco CallManager installation. One or more CTIManagers can be 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.

In previous releases, applications connected to a single Cisco CallManager in a cluster. Under this structure, an application could only access the resources and functionality in that Cisco CallManager. As a result, a single Cisco CallManager failure was catastrophic to an application. In addition, when resources in a failed CallManager rehomed to another CallManager in the cluster, those resources became unavailable to the application until these resources rehomed to the Cisco CallManager to which the application had connected.

With the addition of the CTIManager in the 3.1 release, applications can access resources and functionality of all Cisco CallManagers in the cluster and have improved failover capability. When a CTIManager fails, the application can access the secondary CTIManager only if the application supports it (for JTAPI apps) or if the Cisco TAPI Service Provider (Cisco TSP) is properly configured (for TAPI apps). For more information about failover and failback, see to the "CTI Redundancy" section on page 34-4.

CTI Controlled Devices

The following three types of CTI control devices exist:

- Cisco IP phones
- CTI ports
- CTI route points

CTI-controlled Cisco IP phones comprise regular phones that a CTI application can control.

CTI ports as virtual devices can have one or more virtual lines, and software-based Cisco CallManager applications such as Cisco SoftPhone, Cisco AutoAttendant, and Cisco IP Interactive Voice Response (IVR) use them. You configure CTI ports through the same Cisco CallManager Administration area as phones. For first-party call control, you must add a CTI port for each active voice line.

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.

Note If you are planning to use a TAPI application to control CTI port devices using the Cisco TAPI Service Provider (TSP), then 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 speed dial and call forwarding.

CTI devices (CTI ports, CTI route points) must associate with device pools containing the list of eligible Cisco CallManagers for those devices. For general instructions on how to configure settings for CTI ports, refer to the "Adding a Phone" section in the *Cisco CallManager Administration Guide*. For general instructions on how to configure settings for CTI route points, refer to the "Adding a CTI Route Point" section in the *Cisco CallManager Administration Guide*. For information on how to configure CTI ports and route points for use with a specific application, such as Cisco SoftPhone, refer to the documentation and online help provided with that application.

When a CTI device fails (during a Cisco CallManager failure, for example), Cisco CallManager maintains media streams already connected between devices (for devices that support this feature). Calls in the process of being set up or modified (transfer, conference, redirect, and so on) are dropped.

CTI Redundancy

CTI provides recovery of failure conditions resulting from a failed Cisco CallManager node within a cluster and failure of a CTIManager. This section describes the failover and failback capabilities of the following components:

- Cisco CallManager
- CTIManager
- Applications (TAPI/JTAPI)

Cisco CallManager

When a Cisco CallManager node in a cluster fails, the CTIManager recovers the affected CTI ports and route points by reopening these devices on another Cisco 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 CallManager. If the Cisco IP phone does not fail over to a different Cisco CallManager, the CTIManager cannot open the phone or a line on the phone. The CTIManager uses the Cisco CallManager group assigned to the device pool to determine which Cisco CallManager to use to recover the CTI devices and phones opened by the applications.

When the CTIManager initially detects the Cisco CallManager failure, it notifies the application (JTAPI/TAPI) that the devices on that Cisco CallManager went out of service. When those devices successfully rehome to another Cisco CallManager, the CTIManager notifies the application that the devices are back in service. If no other Cisco CallManager in the group is available, the devices remain out of service.

When a failed Cisco CallManager node comes back in service, the CTIManager rehomes the affected CTI ports/route points to their original Cisco 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 be done for a long period, especially for route points that can handle many simultaneous calls.

Applications may specify to prevent the recovery of CTI-controlled devices that include route points, CTI ports, and IP phones. If an application prevents the recovery of these devices, the CTI ports and route points close when a Cisco CallManager fails. The application also loses control of the CTI-controlled IP phones; however, this does not affect the ability of the phone to rehome to another Cisco CallManager.

If none of the Cisco CallManagers in the Cisco CallManager group is available, the CTIManager waits until a Cisco CallManager comes into service and tries to open the CTI device again. If for some reason the Cisco 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 connected to the CTIManager can recover the affected resources by reopening these devices on another CTIManager. An application determines which CTIManager to use based on the CTIManagers 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 previously opened. An application can reopen a Cisco IP phone before the phone rehomes to the new Cisco CallManager; however, it cannot control the phone until the rehoming is complete.

Note The applications do not rehome to the primary CTIManager when it comes back in service. The applications do not rehome to the primary CTIManager when it comes back in service. Applications failback to the primary CTIManager if you restart the application or if the backup CTIManager fails.

Application Failure

In the CTIApplicationHeartbeatTime parameter, 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 a application (TAPI/JTAPI or an application directly connected to the CTIManager) fails, the CTIManager closes the application and redirects unterminated calls at CTI ports and route points to the application configured call forward on failure (CFOF) number. The CTIManager also routes new calls into CTI ports and route points an application does not open to the application CFNA number.

CTI Configuration Checklist

Table 34-1 provides steps to configure Cisco CallManager for CTI applications.

Table 34-1 CTI Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Add and configure CTI route points or ports for each CTI application.	Adding a CTI Route Point, *Cisco CallManager Administration Guide* Adding a Phone, *Cisco CallManager Administration Guide*
Step 2	Configure the directory number for the CTI device.	Adding a Directory Number, *Cisco CallManager Administration Guide*
Step 3	Install and configure your applications.	Refer to the documentation provided with your application.
Step 4	Configure the appropriate CTIManager and Cisco CallManager service parameters.	Updating a Service Parameter, *Cisco CallManager Administration Guide*
Step 5	Restart the CTIManager service.	Starting and Stopping Services, *Cisco CallManager Administration Guide*
Step 6	Check the CTI In Use check box on the User Configuration pane for the user associated with the application.	Adding a User, *Cisco CallManager Administration Guide*
Step 7	Ensure that you assign devices to the application (identified as a user) that is to control the devices.	Associating Devices to a User, *Cisco CallManager Administration Guide*
Step 8	Ensure that you associate all devices to be used by the application with the appropriate Cisco CallManager group (via the device pool).	Adding a Device Pool, *Cisco CallManager Administration Guide*

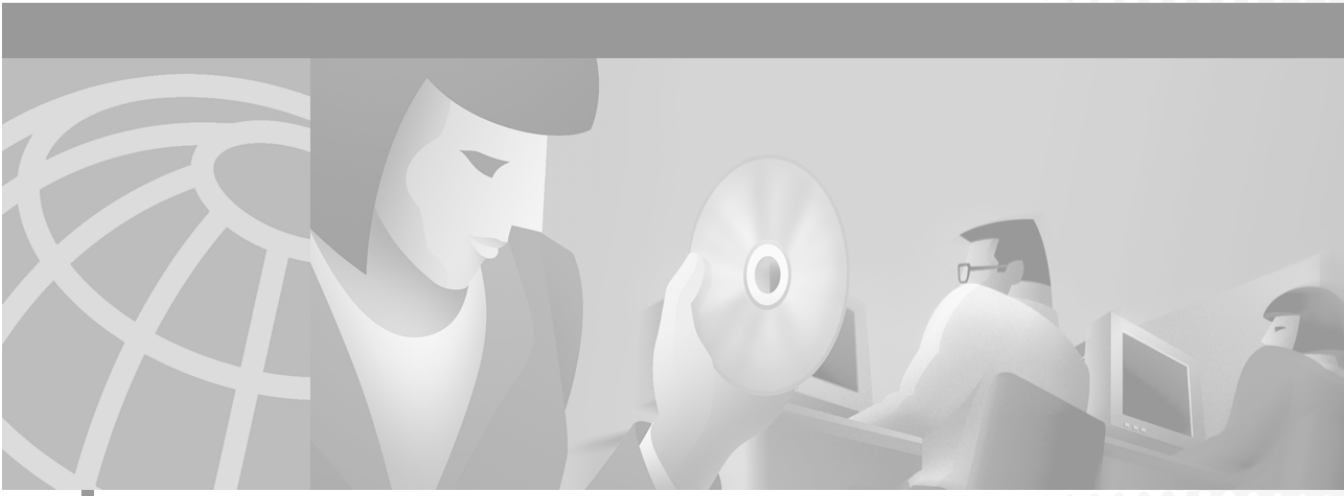
Where to Find More Information

Related Topics

- Services, page 10-1
- Redundancy, page 6-1

Additional Cisco Documentation

- *Cisco JTAPI Developer Guide*
- *Cisco TAPI Developer Guide*
- *Cisco CallManager Serviceability Administration Guide*



PART 9

System Maintenance

CHAPTER 35

Administrative Tools Overview

This section provides an overview of the following tools for Cisco CallManager administrators:

Bulk Administration Tool (BAT)

The Bulk Administration Tool (BAT), a plug-in application to Cisco CallManager, lets you add, update, or delete a large number of phones, users, Cisco VG200 gateways and ports, and Cisco Catalyst 6000 24 Port FXS analog interface modules to the Cisco 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 is a web-based application that requires Internet Explorer 4.01 Service Pack 2 or later or Netscape 4.5 or later. Cisco CallManager Administration provided the model for the look and feel of BAT.

You can access BAT from Cisco CallManager Administration and vice versa using the **Application** menu.

For more information on BAT, refer to the *Bulk Administration Tool Guide for Cisco CallManager.*

Administrative Reporting Tool (ART)

The Administrative Reporting Tool (ART) for Cisco CallManager 1.0(1), a web-based reporting application, generates the following reports that provide information regarding voice quality and generates reports on the gateway performance.

- Quality of service
- Traffic details
- User call details
- Billing details
- Gateway details
- Call Detail Records

The Cisco CallManager records information regarding each call in Call Detail Records (CDRs) and Call Management Records (CMRs). CDRs and CMRs serve as the basic information source for ART and are stored in the ART database.

Retrieve the information that is not present in the CDR and CMRs, but is required for various reports, from the Light Weight Directory Access Protocol (LDAP), or the ART administrator must enter the information.

Access to ART is available only through a secured login to the package. The user ID and password for ART access are the same as the user profile set for Cisco CallManager.

Access ART using Internet Explorer 4.01 Service Pack 2 or later, or Netscape 4.5 or later.

To view the reports, ART requires the Adobe Acrobat reader, which you can download and install from the ART main screen.

For more information on ART, refer to the *Administrative Reporting Tool Guide for Cisco CallManager.*

Remote Serviceability for Cisco CallManager

Network management tools, if properly deployed, can provide the network administrator with a complete view into any enterprise network. With the advent of converged networks, it is imperative to have network management systems enable the following capabilities, at a minimum:

- Network discovery and topology maps
- Inventory control and configuration management of networked nodes
- Report generation, system logging, and analysis of the respective data

Cisco CallManager Remote Serviceability and CiscoWorks2000 provide the above capabilities, as well as other mechanisms, which enable visibility into the health and availability of the Cisco AVVID network. Considerable management features have been added, starting with Cisco CallManager Release 3.0, to permit visibility into the operation and reporting capability of a Cisco AVVID network. Table 35-1 lists the features that have been provided for network management applications to export data and, particularly for CiscoWorks2000, to provide reporting, proactive management, debugging, and other capabilities.

Table 35-1 Remote Serviceability Features for Cisco CallManager

Feature	Description
Simple Network Management Protocol (SNMP) Instrumentation	Two Management Information Bases (MIBs) have been added to Cisco CallManager to permit a network management system to extract appropriate information.
Call Detail Record (CDR) Logging	Call Detail Record is used for accounting, debugging, and path analysis.
Cisco Discovery Protocol (CDP) Support (CDP MIB)	Cisco Discovery Protocol support for Cisco CallManager server advertisement and discovery via a network management system such as CiscoWorks2000. This is the “tell” side of CDP via SNMP enablement.
System Logging Components	Cisco Syslog Collector for message filtering, collection, and repository to a Syslog server.

The following sections describe some of these features in more detail.

SNMP Instrumentation on the Cisco CallManager Server

Simple Network Management Protocol (SNMP) features for Cisco CallManager enable network management applications to retrieve data from the Cisco CallManager server in a standard fashion. The SNMP agent on the Cisco CallManager server is a subagent (extension agent) of the Microsoft Windows 2000 system agent. Therefore, you must enable the SNMP service on the Windows 2000 system for the SNMP instrumentation to function on the Cisco CallManager server.

Two Management Information Bases (MIBs) were introduced in Cisco CallManager Release 3.0 to permit the export of data as well as to support server advertisement and discovery. Both MIBs are extension agents and are independent of each other to facilitate future applications and functionality:

- CISCO-CCM-MIB

  This MIB exports data from the Cisco CallManager database and other data sources. Examples of the exported data include Cisco CallManager group tables, region tables, time zone group tables, device pool tables, phone detail tables, gateway information tables and status traps, CDR host log table, performance counters, and so on.

- CISCO-CDP-MIB

  This MIB uses Cisco Discovery Protocol (CDP) to enable CiscoWorks2000 to discover the Cisco CallManager server and to retrieve information from variables such as the interface table, deviceID, and so on. This is a limited implementation of the MIB and is essentially a subset of the CDP MIB related to advertisement (that is, the "tell" side of the MIB).

  More detailed information on the CDP MIB is available on Cisco Connection Online (CCO) at

http://www.cisco.com/univercd/cc/td/doc/product/fhubs/fh300mib/mibcdp.htm

System Logging Components

The primary objective of system logging components is to provide a working solution for a centralized event logging and debug trace scheme in the multiplatform, distributed Cisco AVVID environment. In an open, distributed

system, you can have multiple applications running on multiple systems. For ease of maintenance, have a common event log and a common trace log where Cisco CallManager can report events.

The interface to log events must be usable with most common programming languages. Also, with a common logging interface, the format of the log messages must be uniform across the system for ease of readability. Finally, the system should also have a common administrative interface to display and control all the event traces. Cisco CallManager and CiscoWorks2000 provide this functionality for unified message logging, display, and management. The following are the two main components to the system logging mechanism:

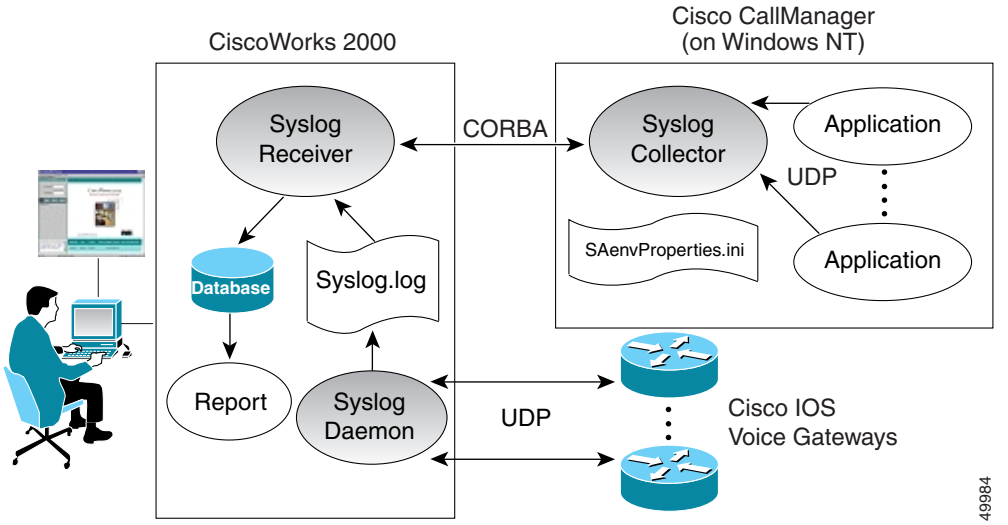
- Syslog Collector, which resides on Cisco CallManager
- Syslog Receiver (The CiscoWorks2000 server can also function as a receiver, as described in the "Syslog Administrative Interface" section on page 35-7.)

Syslog Collector

A Syslog Analyzer Collector (SAC) program runs as a Windows NT service on the Cisco CallManager server or any processing node in the network. The SAC program uses a configuration (.ini) file to set the environment variables such as the CiscoWorks2000 hostname and other parameters. This configuration file, SAenvProperties.ini, and its directory path are specified in the Windows NT registry, and the Cisco CallManager installation program sets their values. During startup time, the SAC tries to check in with the CiscoWorks2000 server to get some configuration and message filter information using a Common Object Request Broker Architecture (CORBA) method call. Then, it sends an initialization message that consists of the SAC hostname, the name of the syslog file, and other information for CiscoWorks2000 to keep track of it.

During normal operation, SAC reads messages from User Datagram Protocol (UDP) port 514. When it receives new messages, SAC processes the messages (for example, by performing filtering and time zone conversions) and then sends them to the CiscoWorks2000 server for storage and analysis. SAC also sends a status or statistic message periodically to the CiscoWorks2000 server. Figure 35-1 illustrates the interoperability of CiscoWorks2000 and Cisco CallManager.

Figure 35-1 Syslog Architecture for the Interoperability of Cisco CallManager and CiscoWorks2000



During installation of Cisco CallManager, the installation program normally prompts you to enter CiscoWorks2000 server information (for example, hostname or IP address). You can skip this step during installation and add the information later by modifying the contents of the file SAenvProperties.ini, located in \Program Files\Cisco\Bin. Set the SAC_SERVER and BINDNAME to the CiscoWorks2000 server.

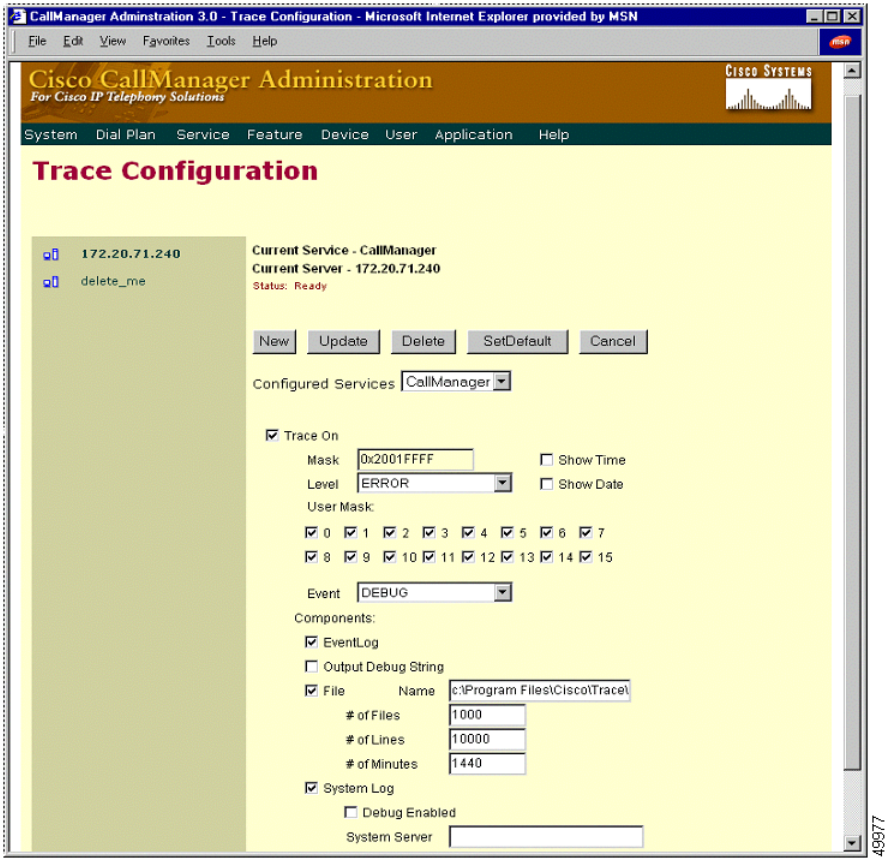
The contents of the SAenvProperties.ini file are as follows:

```
FILE= /var/log/syslog_info
SAC_PORT = 514
SAC_SERVER=<your_server_hostname.your_domain>
SAC_SERVER_PORT = 42342
VERSION = 1.1
BINDNAME =<your_server_hostname>::SaReceiver
DEBUG_LEVEL=4
SA_APP_NAME=SyslogAnalyser
```

Syslog Administrative Interface

The Syslog administrative interface is a web-based interface that is part of Cisco Call Manager Administration, under **Service** > **Trace**. A new page shows the status of each trace flag and the trace output options of each service for each server in a Cisco CallManager cluster, as illustrated in Figure 35-2. You can enable or disable the trace flags from the administrative interface, which updates the trace configuration in the database layer.

Figure 35-2 Administrative User Interface for Syslog Trace Functions



Options also exist to enable the debug trace messages and to configure the Syslog server name. You should enable the debug trace message option only when there is little activity in the system. This method avoids putting excessive traffic on the network and lessens the burden on the system. You can send the debug trace messages to the Windows 2000 EventLog, to a local file, to the Syslog server, or to all three. Enter the Syslog server name only when using a syslog daemon other than the CiscoWorks2000 SAC as the Syslog server. Otherwise, leave the Syslog server name blank, and it will default to the local host name.

CiscoWorks2000 Voice Management Features

CiscoWorks2000 is a suite of products for network management, inventory control, analysis, and debugging. The Common Management Framework (CMF) in CiscoWorks2000 is a web-based application with various plug-in application suites that provide certain management feature sets.

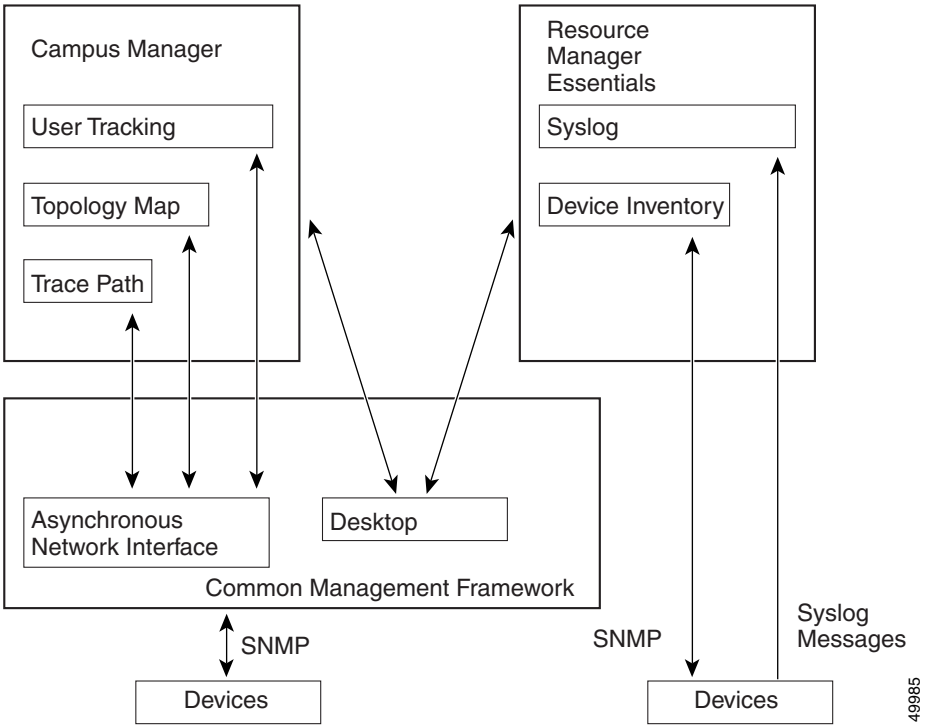
Each application suite in the common web-based interface takes advantage of a common database. CiscoWorks2000 can run on either Windows NT or a Sun Solaris platform. Table 35-2 describes the respective components needed to complete the product suite for Cisco AVVID network management.

Table 35-2 Components of CiscoWorks2000 Product Suite

CiscoWorks2000 Components	Description and Function
Common Management Framework Release 1.1.1 (CD-ROM One, edition 3)	Serves as baseline web application for all components, single GUI manager for other CiscoWorks2000 components, and central database. This component is part of the LAN Management Solution (LMS) bundle.
Campus Manager Release 3.0.1 P1 (included with Voice update)	Provides various functionality such as discovery and topology map, central point for host management (console), user tracking, and path analysis.
Resource Manager Essentials Release 3.2 (included with Voice update)	Maintains the managed device inventory, configuration management, and system logging repository and analysis.

As mentioned, the CiscoWorks2000 architecture consists of a Common Management Framework (CMF) with a web-based desktop as a single point of management. An additional component, the asynchronous network interface (ANI), provides data collection services using Simple Network Management Protocol (SNMP), Cisco Discovery Protocol (CDP), and Interim Local Management Interface (ILMI) tables. Figure 35-3 illustrates this architecture.

Figure 35-3 CiscoWorks2000 Architecture



Discovery of the network occurs when you provide a seed device, preferably a router or a switch, through which the ANI can discover the network by reading its neighbors' CDP cache tables and SNMP variables, and can build a network topology map accordingly. The CMF also provides granular security, process control, and device information retrieval via SNMP. It uses CDP and the Cisco CallManager Management Information Bases to discover the Cisco CallManagers on the network and to retrieve and store their appropriate data tables.

Campus Manager

The ANI discovery process added the support for voice components of the Cisco AVVID network in Common Management Framework (CMF) Release 1.1.1. This CMF release supports the following voice devices and functions:

- Cisco CallManager

  Cisco CallManager Release 3.0 (and later) contains the CDP driver, and it supports partial CDP MIB and SNMP. This is the “tell” side of CDP, so it is always an edge device, and it displays as a Cisco CallManager icon in the topology map.

- Cisco IOS voice gateways

  The voice gateways are discovered in the same way as regular routers.

- Cisco IP Phones (models 7960, 7940, and 7910)

  Cisco IP Phones contain the “tell” side of the CDP driver, but they do not support SNMP.

- VLAN management

  This feature provides tools for graphical VLAN configuration and logical topology mapping.

- End-station mobility and tracking

  This feature provides tools for mobile user and dynamic VLAN tracking and configuration.

- Trace path analysis

  This feature traces Layer 2 and Layer 3 paths between two devices or end stations using IP address or directory number.

Because there are usually many Cisco IP Phones installed on a network, the ANI must handle the discovery of Cisco IP Phones separately to avoid overcrowding the network topology map. For this reason, CMF Release 1.1.1 ignores the CDP cache entries of the Cisco IP Phones in the neighboring switches and does not create any device objects for them; hence, daisy-chained IP phones are not discovered. The Cisco IP Phones are treated as end user devices and are discovered through User Tracking discovery, as described in the next section.

User Tracking

User Tracking (UT), a service module of the Campus Manager and ANI, specifically discovers end user nodes such as systems, Cisco CallManager hosts, Cisco IP Phones, and non-CDP systems as well. User Tracking performs an initial discovery of all hosts in the topology map and a subsequent discovery to maintain the user tracking table. You can specify a time limit for this subsequent discovery, and the default is 1 hour.

The initial UT discovery performs the following steps to generate a phone table:

1. UT reads the Content Addressable Memory (CAM) and Address Resolution Protocol (ARP) table of the switches and routers that have already been discovered by ANI and recorded in the topology map.
2. Based on information from CAM and ARP queries, UT generates an end-user table with device and port information. If the end user is a Cisco IP Phone, UT performs the following steps:
   - It reads the phone entry from the CCM hosts, using the management information base CISCO-CCM-MIB.
   - It generates a phone table that corresponds to values.
   - For older models of Cisco IP Phones (Cisco IP Phone models 12 SP+ and 30 VIP), UT uses the CCM-MIB to query Cisco CallManager, and it builds the phone table based on the device and port information gathered from the initial discovery.

Note For non-Cisco IP phones, query is made to Cisco CallManager via SNMP, and the returned information is cross-referenced with information obtained from standard queries made to switches to get MAC addresses and switch ports (query of CAM table) and from queries made to routers to map IP addresses to MAC addresses (query of ARP cache).

Trace Path Analysis

The Path Analysis tool, a part of the Campus Manager, traces IP connectivity between any managed devices in the network. The end points of the trace must be a managed device or end-user node in UT because there is a heavy reliance on accurate information for the trace to be performed. The trace displays end-to-end

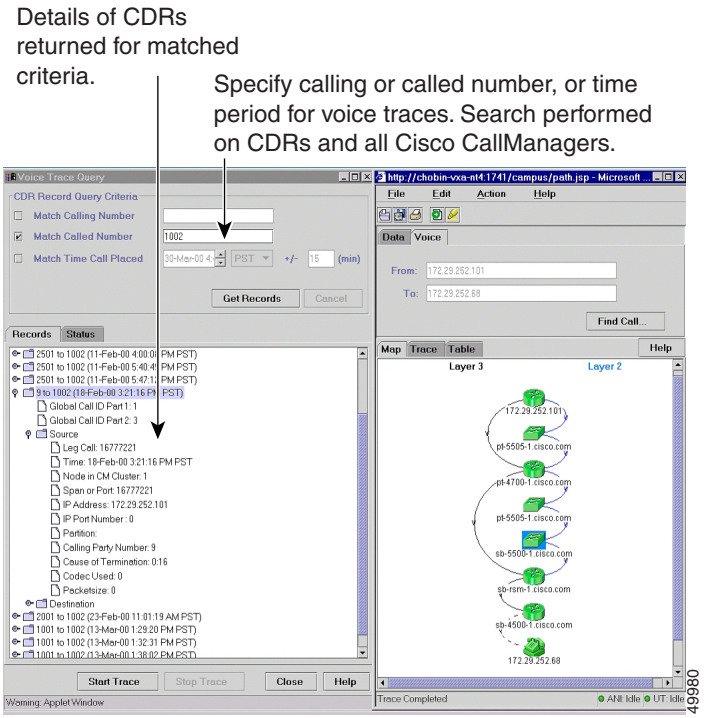
Layer 3 (IP) paths and, in some instances, the Layer 2 devices within the Layer 3 path. The Path Analysis tool offers two types of traces, data and voice. This chapter discusses only the voice trace.

A voice trace is performed using the call detail records (CDRs), and it also displays the IP path of the trace in case there is a need to discover the state of the network between two phones or between a phone and Cisco CallManager. The data path map can also display a reverse path, which is used if there is congruency in the Layer 3 IP routing paths. The non-CDR voice trace also performs a source-routed trace using the same IP precedence value as a voice call (RTP only). This trace is used if voice follows a different path than data and if it can take advantage of, or detect any problems with, any QoS that has been provisioned for voice.

The CDR-based voice trace can accept three values for a trace: time period to match the call, calling number, and called number. Matching of the data occurs with the right-most digits entered. The path analysis tools search the CDRs of all the managed Cisco CallManager hosts in the database, and matched records are returned. The tools can display and examine the records with best-effort suggestions for possible causes of a problem and corrective actions.

Figure 35-4 shows an example trace path analysis, with Layer 2 and Layer 3 devices displayed.

Figure 35-4 Example Trace Path Analysis



Resource Manager Essentials

The CiscoWorks2000 LAN management solution is also bundled with the Resource Manager Essentials (RME), which are primarily responsible for inventory control, system configuration repository and configuration management, syslog server and syslog analysis, and other reporting functions. RME Release 3.1 is the minimum release that supports detailed reporting capabilities and manageability for Cisco CallManager hosts that are imported.

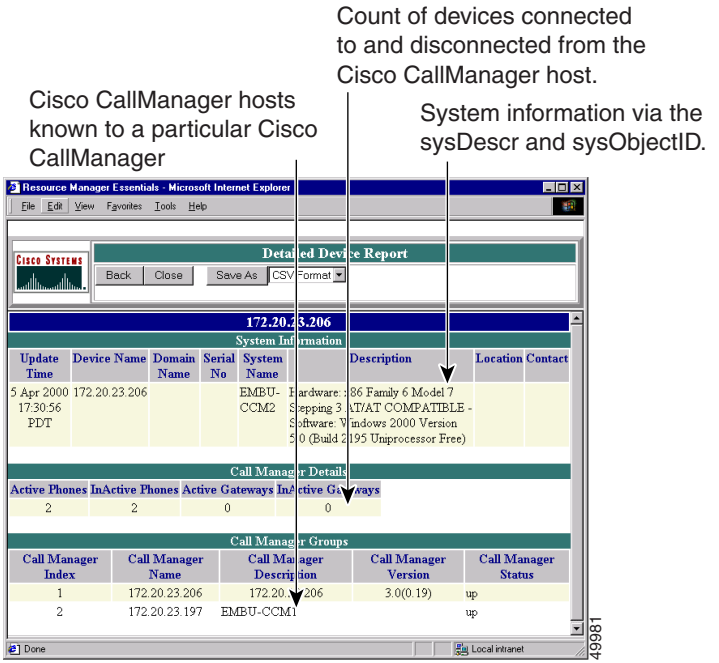
System logging capabilities of Cisco CallManager, described in the "System Logging Components" section on page 35-4, are well integrated with CiscoWorks2000. RME serves as a single point of management for Syslog Collector message filter configuration and device detail reporting for Cisco CallManager and other Cisco managed devices.

Inventory Control and Reporting

Cisco CallManager is supported in RME in the same manner as any Cisco device. The MIBs supported by Cisco CallManager are accessible through a standard SNMP agent. RME identifies the Cisco CallManager via the Compaq sysObjectID, so it is imperative to avoid exporting a similar system that is not running Cisco CallManager; otherwise, RME will waste resources by periodically collecting configuration information from the non-CallManager system.

RME also creates a separate group in the device selector (a new system view named "Cisco CallManagers") once it detects that Cisco CallManager hosts have been imported for inventory and reporting management. Reports exposed for the device selector are intended to show data about the configuration and state of Cisco CallManager itself, and they do not report on information regarding the individual components configured on Cisco CallManager. Figure 35-5 shows an example device report from RME.

Figure 35-5 Example Device Report from RME



RME also supports report of Multi-Service Port Report (MSP). Essentially, RME evaluates, and the MSP report displays, all the managed Catalyst 4000 and 6000 switches that have inline power modules installed as well as their available ports for IP phone deployment.

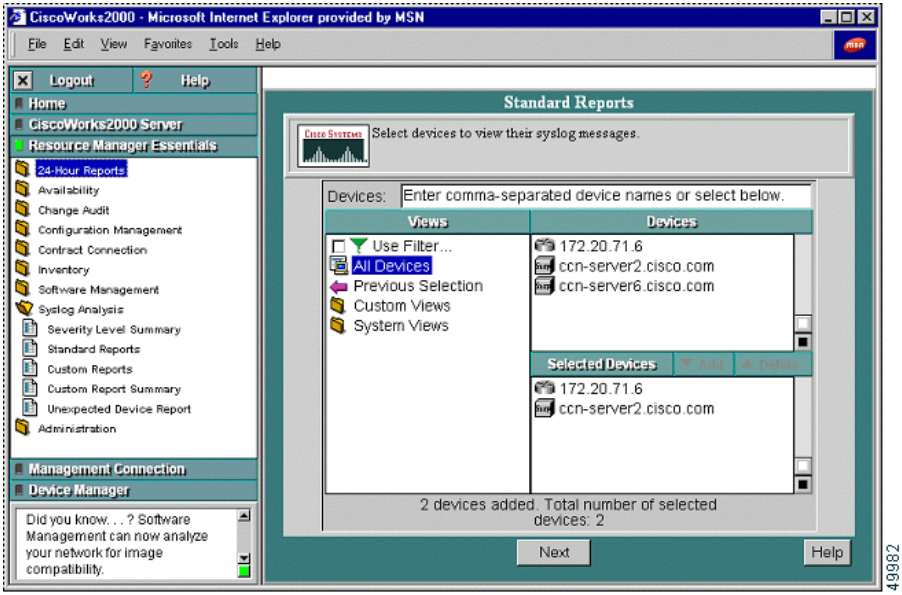
System Logging Management

The server side (RME) of CiscoWorks2000 provides a web-based administrative interface to display the Syslog report from all of the devices in the managed network. There are two types of Syslog reports:

- Standard Report
- Unexpected Device Report

Any devices that support MIB II SNMP variables can be added to the device list of the CiscoWorks2000 configuration, and they are considered as managed devices. The Syslog messages from these managed devices are collected in the Syslog Standard Report. On the other hand, the Syslog messages from the unmanaged devices all go to the Unexpected Device Report. Figure 35-6 shows the administrative user interface for the Standard Report.

Figure 35-6 Standard Report in CiscoWorks2000



You can also use the administrative interface of CiscoWorks2000 to define custom reports such as user URL, automated action, and message filters (as shown in Figure 35-7). These features of the Syslog Analyzer and the administrative interface were updated in RME Release 3.1 to support Cisco CallManager and its suite of voice applications.

Syslog Message Filtering

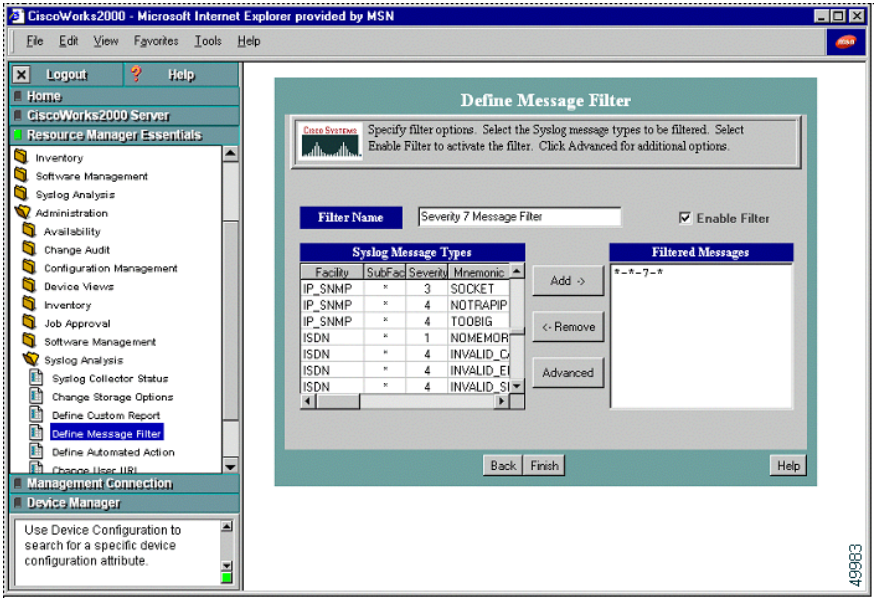
In addition to System Diagnostic Interface (SDI) filtering, there are two places in the Syslog Analyzer where you can perform message filtering:

- In the Syslog Analyzer Collector (SAC) process, before the message is sent to the network
- In the CiscoWorks2000 server, where the administrator can define a custom report

Note If you set the Syslog filters on the CiscoWorks2000 server, all defined Syslog messages are sent to the server, thus creating erroneous network traffic. Cisco recommends that you use the SAC to create filters prior to sending them to a Syslog server.

The filtering mechanism allows you to define filters that are based on the source, the facility code, the subfacility codes, severity levels, mnemonic codes, or patterns in the message. Figure 35-7 shows an example of defining a message filter in the CiscoWorks2000 administrative interface.

Figure 35-7 Message Filter Defined for a Remote SAC



Alarms

The Syslog Analyzer in CiscoWorks2000 has a web-based administrative interface to define an automatic action for a set of events or Syslog messages from particular devices. In future releases of CiscoWorks2000, this feature will be

enhanced further to generate alarms or traps. Currently, the Syslog Analyzer can be used for event notification via either writing to a log file or generating an e-mail message. Cisco recommends that you configure the appropriate e-mail destination, whether that be to some e-mail receiver that can generate a page or to some Network Operation Center (NOC) alert e-mail alias. From an operational perspective, there would be a clear advantage to having event notification e-mails sent to an e-mail capable pager or cellular phone.

Call Detail Records

When CDR collection is enabled, Cisco CallManager writes call detail records (CDRs) to the SQL database as calls are made. CDR collection is enabled and configured through service parameters that are set in Cisco CallManager Administration. You must enable CDR collection on each Cisco CallManager in the cluster for which you want to generate records (see the "CDR-Related Service Parameters" section on page 35-20

All CDR records are written to the local database on each Cisco CallManager and then moved from the local database to the publisher database for the cluster in a low priority thread at 1-minute intervals.

If the local database is not available, then they are written to any of the other subscriber databases in the cluster. When the local database becomes available, the writing of new records resumes on the local database.

Enabling CDR Collection

CDR collection is enabled through a Cisco CallManager service parameter named CdrEnabled. To enable CDR collection:

1. Open Cisco CallManager Administration.
2. Select **Service > Service Parameters**.
3. Click on the Cisco CallManager server on which you wish to enable CDR collection.
4. Select Cisco CallManager from the list of configured services.
5. Select CdrEnabled from the list of service parameters.

6. Choose T (true, CDRs enabled) or F (false, CDRs disabled) from the Value drop-down list box.
7. Repeat this procedure on each Cisco CallManager in the cluster. You do not need to restart the CallManager for the change to take effect.

CDR-Related Service Parameters

The following tunable service parameters apply to CDRs:

- MaxCdrRecords—Cisco TFTP service parameter that controls the maximum number of CDRs on the system. When this limit is exceeded, the oldest CDRs are automatically removed, along with the related CMR records, once a day. The default is 1.5 million records.
- CdrEnabled—Cisco CallManager service parameter that controls whether or not CDRs are generated.
- CdrLogCallsWithZeroDurationFlag—Cisco CallManager service parameter controls whether calls with zero duration are logged in CDRs. The default is False (zero duration calls not logged).

Removing CDR Records

The CallManager application relies on post-processing applications such as ART or other 3rd-party packages to analyze CDR data. The removal of the CDR data should be done by the administrator when all post-processing applications are through with the data. Because this involves modifying the database, the SQL user CiscoCCMCDR should be used.

If CDR records accumulate to a configured maximum (as set by the MaxCdrRecords service parameter, which defaults to 1.5 million records), then the oldest CDR records are removed along with related CMR records once a day.

When removing CDR data after analysis, be sure to remove all related CMR records also.

Tips It is best to remove CDR and CMR records often instead of once a day or week in a large system. Queries to remove records can consume CPU time and transaction log space relative to the size of the table. The smaller the table, the quicker the query. Large queries on a live database can adversely affect call processing.

CDR Database Access

The easiest way to read data from the SQL database is to use ODBC. A good connection string would look like one of the following examples depending on whether you need to get to the configuration data or CDRs:

DRIVER={SQL Server};SERVER=machineX;DATABASE=CCM0300

DRIVER={SQL Server};SERVER=machineX;DATABASE=CDR

Be sure to use the correct database name. Previous versions of the product had the CDR tables in the CCM0300 database. The tables have been moved to the CDR database. Also, you will need access to both the configuration database and CDR database to properly resolve the CDR information.

The machine that is the central collector of the CDR information is the machine serving the primary CCM0300 database. To determine the publisher database (machine and name) currently in use by the cluster

1. Choose **Help > About Cisco CallManager**.
2. Click the **Details** button.

   The Database field in the Database Information area displays the name of the Cisco CallManager server that is the publisher database for the cluster.

Access to CDR records is controlled through SQL Users. Table 35-3 specifies the UserID and password that should be used when accessing the Cisco CallManager database.

Table 35-3 SQL Users for CDR Access

Database	Tables	SQl UserID	Password	Capability
CDR	CallDetailRecord, CallDetailRecordDiagnostic	CiscoCCMCDR	dipsy	Read/write access to CDR Read access to CCM0300
CCM0300	All	CiscoCCMReader	cowboys	Read only

Where to Find More Information

Related Topics

- Cisco TFTP, page 8-1
- Understanding Cisco WebAttendant, page 30-1
- Understanding Voice Gateways, page 32-1
- Cisco IP Phones, page 33-1
- Call Admission Control, page 7-1
- System Configuration Checklist, page 4-11

Additional Cisco Documentation

- Device Defaults Configuration, *Cisco CallManager Administration Guide*
- Device Pool Configuration, *Cisco CallManager Administration Guide*
- Gateway Configuration, *Cisco CallManager Administration Guide*
- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Cisco CallManager Group Configuration, *Cisco CallManager Administration Guide*
- Cisco JTAPI Installation and Configuration, *Cisco CallManager Administration Guide*

- *Bulk Administration Tool Guide for Cisco CallManager*
- *Administrative Reporting Tool Guide for Cisco CallManager*

CHAPTER 36

Administrative Accounts and Passwords

This section provides descriptions and guidelines for administrative accounts and passwords on a Cisco CallManager system. It covers the following topics:

Administrator Account

This is the default Windows NT administration account. This password is not used by Cisco CallManager. This password can be different on Cisco CallManager servers only if it is not used to access Cisco CallManager Administration.

CCMAdmin Account

This account is installed so that Cisco CallManager Administrators can use it to access Cisco CallManager Administration web pages.

- The password for this account should be the same on all servers in a Cisco CallManager cluster.
- The account should have administrative privileges on each machine in the cluster in order to support the Serviceability Control Center web pages. This allows the IIS server to perform passive authentication for starting and stopping services and for database replication.

SQLSvc Account

The SQLSvc account is the core account used for server-to-server interaction within a Cisco CallManager system. This account must be the same on every machine in the cluster for database replication to work properly.

Changing the SQLsvc Password

If the SQLsvc password has been changed on the publisher from the installed default, replication of the publisher database will fail when a new subscriber is added.

If replication has failed, change the new subscriber's SQLsvc service password to match the SQLsvc password on the publisher, and replication should succeed.

SQL Server Administration (sa) Account

This is the default SQL Server administration account. This password is only used by installation and migration. Most of the system does not use this account.

Where to Find More Information

Related Topics

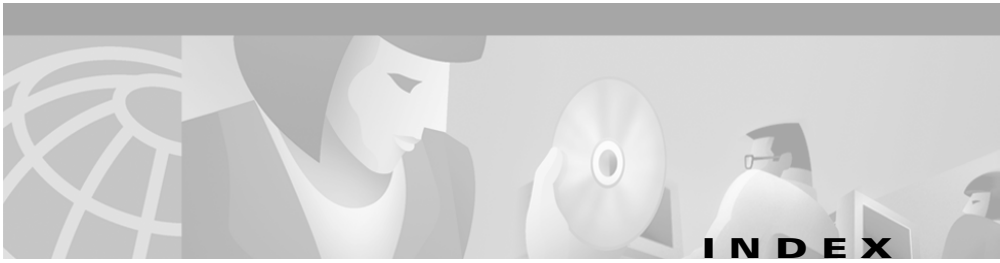
- Cisco CallManager Groups, page 4-1
- Call Admission Control, page 4-10

Additional Cisco Documentation

- Cisco CallManager installation and upgrade documents for the specific release of Cisco CallManager installed on your system

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_0/install/

- Service Parameters Configuration, *Cisco CallManager Administration Guide*
- Starting and Stopping Services, *Cisco CallManager Administration Guide*
- *Installing Cisco CallManager 3.1*
- *Cisco CallManager Serviceability Administration Guide*



A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W