Installation and Administration Guide for the Cisco TelePresence Exchange System Release 1.1

Revised July 19, 2012

Americas 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: 408 527-0883

Installation and Administration Guide for the Cisco TelePresence Exchange System Release 1.1

CONTENTS

Preface

This preface contains the following sections:

Audience

This guide is for experienced network administrators who are responsible for installing, configuring, and maintaining the Cisco TelePresence Exchange System.

Purpose

The *Installation and Administration Guide for the Cisco TelePresence Exchange System* provides information about how to install, configure, maintain, troubleshoot, and upgrade the Cisco TelePresence Exchange System.

Organization

This guide includes the following parts:

Part	Contents
Overview	Provides an overview of the Cisco TelePresence Exchange System and its user interfaces.
Installing the Cisco TelePresence Exchange System	Describes how to install the Cisco TelePresence Exchange System software, synchronize the database servers, and upgrade the software.

Part	Contents
Configuring the Cisco TelePresence Exchange System	Describes how to configure the Cisco TelePresence Exchange System.
Configuring External Network Components for the Cisco TelePresence Exchange System	Describes how to configure the solution components, which provide the signaling, media services, scheduling, and other functions that enable the Cisco TelePresence Exchange System to deliver an end-to-end solution.
Maintaining the Cisco TelePresence Exchange System	Describes how to set up the system for proper maintenance and how to perform maintenance tasks.
Troubleshooting the Cisco TelePresence Exchange System	Describes how to troubleshoot and recover from problems.
Appendixes	Provides an installation worksheet and reference information about supported commands, product-specific MIBs, and data migration. Also includes conceptual information on organization bandwidth, endpoint capacity, protocols, and bridge selection.
Glossary	Defines terms that are related to the Cisco TelePresence Exchange System that might not be commonly known.

Conventions

This publication uses these conventions to convey instructions and information:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords or tabs are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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

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

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

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

Related Documentation

To access the documentation suite for the Cisco TelePresence Exchange System, go to the following URL: http://www.cisco.com/go/ctx-docs

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

PART 1

Overview of the Cisco TelePresence Exchange System

CHAPTER 1

Product Overview

Revised July 3, 2012

The Cisco TelePresence Exchange System is an integrated video service-creation platform that enables service providers and strategic partners to offer secure cloud-based managed and hosted Cisco TelePresence and business video services. The Cisco TelePresence Exchange System is a software environment that simplifies end-to-end subscriber service provisioning; optimizes intelligent call routing for endpoints and network bandwidth; manages the call processing and allocation of media resources for conferencing; consolidates a centralized control point for management, billing, and administration; and presents an open application programming interface (API) for application integration such as scheduling and directory services.

Based on proven technology and powered by a fully redundant and horizontally scalable architecture, it delivers an open, scalable, and robust multi-tenant solution that can grow in scale and functions based on service needs. As a result, it accelerates time to market by simplifying the process of setting up new services and promotes service innovation through APIs that support service customization and partner on-boarding.

The following sections provide additional information about the Cisco TelePresence Exchange System:

Benefits

The Cisco TelePresence Exchange System provides the following benefits to service providers:

- Secure and scalable network-based telepresence services for inter-company conferencing.
- Call admission control and network bandwidth management for inter-company point-to-point meetings.
- A standard interconnect architecture across service providers to facilitate peering.
- Interoperability with legacy video systems to expand the service footprint.
- Organization ports functionality to manage network utilization on a per-customer basis.

- Open application programming interfaces (APIs) to create service differentiation (for scheduling portals and vertical applications) and to facilitate integration with existing billing and operational support systems.
- Call-detail records (CDRs) for calls that are placed on the system, including direct-dial calls between two enterprises that are hosted by the same service provider and direct-dial calls to other service providers. For intra-company direct-dial calls, you can configure the system to pull CDRs from Cisco Unified Communications Manager and generate them locally as if the calls had been processed by the system itself.

Network Architecture

This section describes the network architecture in which the Cisco TelePresence Exchange System operates, and includes the following topics:

Overview

The Cisco TelePresence Exchange System manages the media resources and the call processing that inter-company telepresence services require. The Cisco TelePresence Exchange System fulfills the following network-level responsibilities:

- Controls the reservation and allocation of media resources.
- Manages the resource usage for organizations.
- Provides connectivity between service provider networks.

The Cisco TelePresence Exchange System consists of a server cluster that is designed to provide carrier-grade availability and reliability. With this implementation, the service provider would typically locate the server cluster in its data center.

To provide Cisco TelePresence services, the Cisco TelePresence Exchange System interacts with the following Cisco platforms:

- **Cisco Session Border Controller (SBC)**—The SBC provides call control and security at the demarcation between enterprises and the service provider. The SBC also provides interconnection to other service providers.

  Session border control is integrated into several Cisco IOS routers. For specific models supported by the Cisco TelePresence Exchange System, see the applicable *Release Notes for Cisco TelePresence Exchange System*, at http://www.cisco.com/go/ctx-relnotes.

- **Cisco Application Control Engine (ACE) appliance**—The ACE appliance provides access control, load balancing, and high availability functionality for the Cisco TelePresence Exchange System server cluster.
- **Cisco TelePresence Multipoint Switch**—The Cisco TelePresence Multipoint Switch is a multipoint control unit that provides media switching for multipoint meetings that involve Cisco TelePresence System endpoints.
- **Cisco TelePresence Media Services Engine (MSE) 8000 Series products**—The Cisco TelePresence MSE 8000 Series products support carrier-class telepresence services. The chassis contains a supervisor module and provides nine slots for optional service modules. The Cisco TelePresence Exchange System uses the following types of service modules:
  - **Cisco TelePresence MCU MSE 8510**—Provides inter-working with single-screen telepresence endpoints that support the SIP, H.323, or integrated services digital network (ISDN) standard.
  - **Cisco TelePresence Server MSE 8710**—Provides inter-working with single-screen and multi-screen telepresence endpoints.
  - **Cisco TelePresence ISDN Gateway (GW) MSE 8321**—Provides inter-working with ISDN endpoints.
- **Cisco Router with Integrated Voice Response (IVR)**—The Cisco TelePresence Exchange System uses the IVR router for calls that have a missing or incorrect meeting PIN and for calls that encounter exception conditions. The IVR plays the appropriate prompts and collects the meeting PIN from the customer.

  IVR functionality is integrated into several Cisco IOS routers. For specific models supported by the Cisco TelePresence Exchange System, see the applicable *Release Notes for Cisco TelePresence Exchange System*.
- **Cisco Unified Communications Manager (Unified CM)**—The Unified CM provides configuration, management, and call routing to configure a set of telepresence endpoints. The service provider Unified CM is used to support hosted endpoint deployments.
- **Cisco TelePresence Video Communication Server**—The Cisco TelePresence Video Communication Server (Cisco VCS) extends face-to-face video collaboration across networks and organizations by supporting any-to-any video and telepresence communications. When an enterprise wants to deploy Cisco TelePresence and third-party standards-based H.323 and ISDN endpoints, the enterprise must install at least one Cisco VCS.
- **Cisco TelePresence Manager**—The Cisco TelePresence Manager provides scheduling integration for a cluster of Cisco TelePresence Multipoint Switch resources, and supports One-Button-to-Push (OBTP) session initiation for endpoints on the Cisco TelePresence Exchange System network.

  When you enable OBTP on an endpoint, the Cisco TelePresence Manager automatically provisions the information that is necessary to allow an endpoint either to directly dial another endpoint with a simple touch of a button, or authenticate and join a scheduled multipoint conference without any need for additional user interaction.
- **Cisco Catalyst Switch**—The switch provides layer 2 and layer 3 connectivity for the Cisco TelePresence Exchange System and the other Cisco platforms. For specific switch models that the Cisco TelePresence Exchange System supports, see the applicable *Release Notes for Cisco TelePresence Exchange System*, at http://www.cisco.com/go/ctx-relnotes.

Cisco TelePresence Exchange System Components

The Cisco TelePresence Exchange System server cluster includes the following components:

- **Administration Server**—Provides the administration console for configuring and maintaining the Cisco TelePresence Exchange System. The administration server also exposes the APIs.
- **Database Server**—Provides a MySQL database for persistent data.
- **Call Engine Server**—Provides SIP call control for the services that are offered by the Cisco TelePresence Exchange System.

Deployment Models

The Cisco TelePresence Exchange System supports the following deployment models:

- **Hosted endpoint service**—For organizations that want the service provider to host the telepresence service. The organization deploys only the telepresence endpoints. The service provider data center contains the Unified CM cluster and Cisco TelePresence Manager components for hosted organizations. Customer endpoints register with the service provider Unified CM.
- **Enterprise endpoint service**—Enterprise endpoint service enables organizations to own and manage the telepresence service within their enterprise network. The enterprise provides the Unified CM cluster and the Cisco TelePresence Manager. Connectivity with the Cisco TelePresence Exchange System uses SIP trunking from the enterprise to the service provider SBC.

  For enterprise deployment of Cisco TelePresence or third-party standards-based endpoints, the enterprise must install at least one Cisco VCS.

Carrier-Grade Availability and Scalability

The Cisco TelePresence Exchange System incorporates the following high-availability features:

- The Cisco TelePresence Exchange System server cluster includes redundant servers for each of the functional components.
- The Cisco Application Control Engine (ACE) provides load balancing to the administration servers and the call engine servers. If one server becomes unavailable, the other server processes the full traffic load. Because ACE provides a single IP address to the server cluster, the service remains available to the users.
- Persistent data is stored in a replicated database on the database servers. If the active database server becomes unavailable, the standby database server becomes active.
- Database backup and restore capability.
- Media resources are provided by clusters of media servers. If a media server becomes unavailable, calls that are using resources on that server are dropped. The remaining active media servers in the cluster handle all new calls.

Licensing

The Cisco TelePresence Exchange System requires the installation of a license to enable Meet-Me, Rendezvous, and direct dial services. The system checks the license before scheduling a meeting or initiating a Meet-Me, Rendezvous, or direct dial call. The system blocks these operations if a valid license is not detected.

The Cisco TelePresence Exchange System comes preinstalled with a 60-day evaluation license. After 60 days, you must install a permanent license to continue to use the Meet-Me, Rendezvous, and direct dial services. The permanent license is perpetual, meaning that it does not expire and does not need to be renewed.

The license is locked to the call engine servers. If you replace a call engine server, you need to request a new license file for the replacement server.

In addition, the use of the active meeting management feature requires a valid active meeting management (ActiveMeetingMgmt) feature license.

Application Programming Interfaces (APIs)

Cisco TelePresence Exchange System includes several application programming interfaces (APIs) that provide provisioning and data access to the system, as follows:

- Scheduling API—Provides web services to enable development of third-party scheduling portals. The scheduling API services allow the portal to schedule and manage Meet-Me, Rendezvous, and two-party direct meetings.

  The Scheduling API also provides “Get” methods for retrieving configured information about endpoints, regions, organizations, whitelist groups, and other objects.

- Active Meeting Management API—Enables real-time management of Meet-Me and Rendezvous meetings that are currently in progress. By using the Active Meeting Management API, you can develop client applications for monitoring and controlling active meetings, typically by concierge or service desk personnel. This API requires a valid ActiveMeetingMgmt feature license.

- CDR API—Provides services to retrieve call detail records from the Cisco TelePresence Exchange System.

For more information on the APIs, see the *API User Guide for the Cisco TelePresence Exchange System Release 1.1*, at http://www.cisco.com/en/US/docs/telepresence/tx/exchange_system/1_1/api_guide/api_guide_11.html .

Key Concepts

Cisco TelePresence Exchange System uses a set of concepts that are described in the following sections:

- Service Providers, page 1-6
- Regions, page 1-6
- Organizations, page 1-6
- Meeting Types, page 1-7
- Service Numbers and Integrated Voice Response (IVR), page 1-7

Service Providers

A service provider offers telepresence services to a set of business customers (organizations) by using media resources that are provisioned at one or more regions in their network.

The Cisco TelePresence Exchange System provides the ability to customize the service greetings and IVR prompts for each service provider.

Regions

A region represents a major geographic region in which a service provider operates.

The region contains one or more resource clusters, which generally include either a Cisco TelePresence Multipoint Switch and/or Cisco TelePresence MSE 8000 Series, Cisco router with integrated voice response (IVR) records, and a Session Border Controller (SBC). A resource cluster is a connected set of resources in one physical data center and is also known as a point of presence (POP).

The system supports multiple points of presence (POPs) within a region—media resources can be configured in more than one data center in a region. All media resources in a region are considered to be equivalent for resource allocation purposes, even if the resources span multiple POPs.

A service provider might have multiple regions configured on a Cisco TelePresence Exchange System, and it is possible for a given region to contain resources for different service providers.

Organizations

An organization is a business customer served by a service provider. An organization controls one or more telepresence rooms (also known as endpoints) that can be included in a meeting. An organization can choose hosted-endpoint service or enterprise-endpoint service.

Meeting Types

The Cisco TelePresence Exchange System supports the following types of meetings:

- **Meet-Me meeting**—A Meet-Me service meeting that is hosted by this Cisco TelePresence Exchange System to provide conferencing for two or more Cisco TelePresence or third-party endpoints. The system reserves and allocates media resources for all of the endpoints in the meeting and provides One-Button-to-Push (OBTP) functionality to the provisioned endpoints. The system also reserves ports of organization bandwidth for the meeting, if applicable.
- **Remote meeting**—A Meet-Me service meeting that is hosted by a remote Cisco TelePresence Exchange System. The Cisco TelePresence Exchange System does not reserve any media resources for a remote meeting. You schedule remote meetings to provide OBTP functionality in the provisioned endpoints and to reserve ports of the organization bandwidth, if applicable.
- **Rendezvous meeting**—Also called a *timeless* or *reservationless* meeting, a Rendezvous meeting is not limited to a single start time. For a Rendezvous meeting, the system starts a new meeting instance and allocates media bridge resources when the first participant joins the meeting. Likewise, the system deallocates resources and ends the current meeting instance when the last participant leaves the meeting.
- **Scheduled two-party direct meeting**—A scheduled direct dialed meeting between two hosted provisioned endpoints. The Cisco TelePresence Exchange System does not reserve any media resources for a direct dial meeting. Two-party direct meetings are scheduled to provide OBTP functionality for those endpoints within the same organization.

Each meeting is associated with a service provider and a region. All media resources for the meeting are allocated from the specified region, even if some participants are from another region or a different service provider. You must specify the region when you schedule the meeting.

If you have the ActiveMeetingMgmt feature license, you can also use the Active Meeting Management collaboration service to make changes to Meet-Me or Rendezvous meetings that are in progress, such as locking or unlocking the meeting to control whether additional participants can join, muting or unmuting participants, increasing the media bridge resource capacity of the meeting, dropping endpoints and redialing them, and increasing the duration of the meeting.

Service Numbers and Integrated Voice Response (IVR)

The service number is the number users call to reach a meeting service such as Meet-Me or Rendezvous. When a user encounters a situation that requires further information or action, such as needing to enter a specific meeting ID, an integrated voice response (IVR) application provides greetings and prompts to collect the information. You configure at least one service number for each service provider on the Cisco TelePresence Exchange System, and you associate a set of IVR prompt files with each service number.

You add IVR prompt sets in the Collaboration Services section of the administration console. When scheduling a meeting, you select a service number for the meeting from among the list of numbers associated with the service provider. Because the service number is tied to a set of prompt files, you can create and use different prompt sets for different meeting scenarios—for example, you can provide prompts for different meetings in different languages.

A Cisco router with IVR provides the IVR services for participants. You configure the router as an IVR resource in the Media Resources section of the Cisco TelePresence Exchange System administration console.

When a participant encounters a situation that requires an IVR prompt, the system forwards the call to the IVR router along with a URL for the prompt. The IVR router sends an HTTP request for the prompt to the system, the system sends a VXML response, and the IVR router plays the prompt audio to the caller.

All meeting participants who interact with the IVR use the prompt set associated with the service number configured for the meeting, including those who dial in by using One-Button-to-Push (OBTP) functionality on their endpoints. If participants attempt to dial a service number that is not associated with the meeting, they hear the prompts associated with the service number that they dialed.

Host PINs for Meet-Me or Rendezvous Meetings

Host PINs enable you to designate a host participant role for a Meet-Me or Rendezvous meeting in order to restrict which participant can start the meeting. More than one participant can be designated as a host. The system categorizes participants as either a host or a guest.

If a guest participant joins the meeting before a host, the system places the participant in a queue and prevents the participant from joining the meeting. Once a host joins the meeting, the meeting starts and all the guests in the queue join the meeting. You can configure whether or not to drop all participants when all the hosts leave the meeting.

You can configure the host settings at the service provider level, organization level, or meeting level. The settings are hierarchical, so you can configure a meeting to inherit its settings from the meeting scheduler organization. In addition, you can configure an organization to inherit its settings from the service provider. If you want a meeting to inherit organization settings, you must enable the inheritance option at the meeting level. Similarly, if you want an organization to inherit service provider settings, you must enable the inheritance option at the organization level.

To use the Host PINs feature, you must enable the host options and create a host personal identification number (PIN) for the meeting. You can choose to have the system generate the host PIN or you can enter a customized host PIN. Host PINs can be reset as many times as needed.

The system designates a participant as a host if one of the following conditions apply:

- A participant manually enters the host PIN when joining the meeting.
- A participant joins the meeting from a provisioned endpoint that has been designated as a host. For this condition, the participant does not need to manually enter a host PIN to join the meeting.

Meeting Extensions for Meet-Me Meetings

When Implicit Meeting Extension is enabled for a Meet-Me meeting, the Cisco TelePresence Exchange System checks for available resources shortly before the two minute end-of-meeting warning. If sufficient resources are available, the system displays a notification indicating to participants that the meeting has been extended, and the meeting continues for a specified length of time. (Participants in meetings hosted on the Cisco TelePresence Multipoint Switch will not see the meeting extension notification, however.)

You can configure the number and length of implicit extensions. The extension length must be in increments of 15 minutes. The maximum number of extensions times the extension length must not exceed 24 hours.

How Implicit Meeting Extension Works

Each time the meeting approaches an extension period, the system checks both currently active and upcoming scheduled meetings to ensure that sufficient resources are available. For example, you can schedule a meeting with a duration of 60 minutes and two 15-minute implicit extensions. The system checks for resources once the meeting has been underway for approximately 58 minutes. If resources are available, the meeting duration is extended to 75 minutes, and the system checks again after the meeting has been underway for approximately 73 minutes. If the extension fails, the system displays the two minute end-of-meeting warning to participants, and ends the meeting after two minutes. Otherwise, the meeting duration is extended to 90 minutes.

You can configure the meeting extension policy at the service provider level, organization level, or meeting level. The policy is hierarchical, so you can configure a meeting to inherit its settings from the meeting scheduler organization. In addition, you can configure an organization to inherit its settings from the service provider. If you want a meeting to inherit organization settings, you must enable the inheritance option at the meeting level. Similarly, if you want an organization to inherit service provider settings, you must enable the inheritance option at the organization level.

Combining Explicit and Implicit Meeting Extension Features

You can also use the Active Meeting Management feature controls to explicitly increase the duration of a Meet-Me meeting that is in progress. You can use both implicit and explicit extensions for the same meeting. After each implicit extension, the system updates the duration of the meeting that is displayed via Active Meeting Management. After each explicit change to the meeting duration, the system resets the number of implicit extensions for the meeting. For example, on an active meeting that was originally scheduled for 60 minutes with two 15-minute implicit extensions enabled, if the system automatically extends the meeting to 75 minutes, and then a service desk user manually changes the meeting duration to 90 minutes, the system could perform two more implicit extensions, if resources are available, for a total duration of up to 120 minutes.

You can use Active Meeting Management to modify the quantity and duration of implicit extensions if implicit extensions were enabled before the meeting began. Changes to the duration of implicit extensions will apply to the next extension period if the system has already checked for resources for an extension or has started the extension. You cannot enable implicit extensions while the meeting is active if they were disabled before the meeting began.

Advanced Resource Management

The Advanced Resource Management feature provides greater flexibility and control of how media bridge resources are allocated for Meet-Me and Rendezvous meetings. This feature introduces the concept of resource groups and reservation types.

Before configuring resource groups or adding Meet-Me or Rendezvous meetings, you must define reservation types. The reservation type determines whether the Cisco TelePresence Exchange System provides a guaranteed or best-effort level of service when reserving a media bridge resource for a Meet-Me or Rendezvous meeting. The reservation type levels of service are defined as follows:

- Guaranteed—When you create a guaranteed Meet-Me meeting, the system reserves media bridge resources for the specified meeting duration. For a guaranteed Rendezvous meeting, the system reserves resources for the meeting that can never be used for other meetings.
- Best-effort—When you create a best-effort Meet-Me or Rendezvous meeting, the system does not reserve any media bridge resources in advance for the meeting. Instead, the system allocates resources when the first participant joins the meeting and deallocates resources when the last

participant leaves the meeting. For a best-effort meeting, the system may fail to allocate resources to the meeting because all the available resources may be in use by other best-effort meetings for the given time period.

When configuring a resource group, you choose a specific service provider and region and one or more reservation types to be associated with the group. You then configure the allowable amount of dedicated media resources and meeting booking capacity for each reservation type chosen. Assigning both a guaranteed and best-effort reservation type to a single resource group allows you to dedicate a specific percentage of the resources to guaranteed meetings and another percentage to best-effort meetings. For best-effort meetings, you have the capability to overbook the media bridge resources. Overbooking assumes that all Meet-Me and Rendezvous meetings associated with a specific reservation type will not be active at the same time. By having different levels of overbookings, you can provide different service levels (for example, Gold, Silver, and Bronze) whereby the higher service levels have lower overbooking and thus have a lower probability of booking failure.

After the resource group has been created, you configure specific media bridge resources to be associated with the group. Based on the set of requirements configured for a Meet-Me or Rendezvous meeting (such as service provider, region, reservation type, and endpoint requirements), the system selects the best-fit resource group and associated media bridge resources to use for the meeting.

Endpoints and Media Profiles

The Cisco TelePresence Exchange System provides telepresence services for Cisco TelePresence System (CTS) endpoints and third-party endpoints. Cisco TelePresence endpoints include both TIP-based endpoints and standards-based H.323 and ISDN endpoints. Supported third-party endpoints only include select single-screen endpoints that are H.323 and ISDN standards-based.

The Cisco TelePresence Exchange System supports the following types of endpoints:

- **Provisioned endpoints**—Endpoints for which all configuration details (such as name, phone number, number of screens, and organization) are known by the administrator and configured on the Cisco TelePresence Exchange System. If an organization has chosen hosted endpoint service, the endpoints are provisioned endpoints.
- **Unprovisioned endpoints**—Endpoints for which limited configuration details are known by the administrator. Through the administration console, you can add unprovisioned endpoints to participate in meetings hosted by the Cisco TelePresence Exchange System.
- **Remote endpoints**—Endpoints for which none of the configuration details are known by the administrator. Remote endpoints are endpoints that join the meeting from another service provider network. Through the administration console, you can add remote endpoints to participate in meetings hosted by the Cisco TelePresence Exchange System.

Media profiles specify the capabilities supported by each type of endpoint that connects to the system, including the type of signalling protocol used when connecting the endpoint to a meeting. They also specify the amount of media resource capacity required for the endpoint. The system includes built-in (pre-defined) media profiles for Cisco endpoints, as well as generic profiles that can be used with most non-Cisco endpoints. You can also add new media profiles.

When you provision an endpoint in the system, you associate it with a specific media profile. The media profiles of the endpoints that you specify when scheduling a meeting determine which types of media bridge resources are capable of hosting the meeting. When more than one type of bridge is capable of hosting a meeting, the Cisco TelePresence Exchange System uses a bridge selection algorithm in order to make optimum use of bridge resources.

For more details on media profiles and the bridge selection algorithm, see the "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection" appendix.

Endpoint Capacity

Three factors determine how many segments the Cisco TelePresence Exchange System reserves for an endpoint: the bridge type that handles the call (Cisco TelePresence Multipoint Switch or Cisco TelePresence MSE 8000 Series), the type of call (dial in or dial out), and the number of endpoint screens.

Note that you can specify at an organizational level that either that the smallest amount of capacity possible will be reserved for endpoints that belong to the organization, or the maximum capacity per endpoint, depending on your needs. If you want an organization to have the flexibility to substitute an endpoint with more screens for an endpoint with fewer screens, you can turn off the Minimize Capacity flag for the organization.

For more details on endpoint capacity calculation, see the "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection" appendix.

Dial Out and Dial In

The Cisco TelePresence Exchange System can dial out to connect provisioned endpoints to a scheduled meeting by using the MUX, TIP, SIP, H.323, or ISDN protocols. The system can dial out to unprovisioned endpoints by using SIP, TIP, H.323 or ISDN. Dial out to unprovisioned endpoints is referred to as Guest Dial Out.

Scenarios in which the system dials out to an endpoint that is configured for dial out include:

- At the start of a meeting, or when the host joins if the Host PINs feature is enabled.
- During an active meeting, at the request of an Active Meeting Management user.
- If the participant is in a meeting, and the resource on which the meeting is allocated fails.
- If the host leaves and later rejoins a Meet-Me meeting and the participant was disconnected because Drop Participants on Host Exit was configured for the meeting.
- If the participant is in a meeting, and the call disconnects abnormally (the endpoint did not hang up, the participant was not dropped from the meeting via Active Meeting Management, and the meeting did not end).

In these dial-out scenarios, the system dials out to the endpoint and attempts to connect for up to 30 seconds, and will retry if necessary up to three more times at 180 second intervals. (If the endpoint rejects a call, the system does not make any further attempts to redial for that scenario.)

The system can accept dial-in calls from endpoints that are using MUX, TIP, SIP, or ISDN protocols. An endpoint can dial in to connect to the meeting by dialing the service number and the conference ID. If the participant dials only the service number, the system sends the call to the IVR service to collect the conference ID. Alternatively, the participant can dial a single digit string, combining the service number and the conference ID with ** in between. For example, for service number 18005551212 and conference ID 12345678, the participant can dial 18005551212**12345678.

One-Button-to-Push (OBTP) functionality is a dial-in scenario; by using the Cisco TelePresence Manager, the system sends the <Service Number>**<Conference ID> string to the endpoint at attend time. When the participant presses the OBTP button, the endpoint dials the string to join the meeting.

For details on protocol selection for dial out and dial in situations, see the "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection" appendix.

Organization Ports Management

Organization ports management is an optional feature which allows each organization to control the number of organization ports that are consumed by telepresence traffic on the network between the organization and the Cisco TelePresence Exchange System.

When you create an organization in the Cisco TelePresence Exchange System, you specify a value for the Max Ports setting, which determines the sum total amount of bandwidth that the organization's endpoints can consume at a given time.

When you create a Meet-Me or remote meeting, you can choose to reserve an amount of organization bandwidth for each endpoint, which counts toward the total organization bandwidth. When the system schedules the meeting, the port requirement for each organization is calculated, based on the endpoints that are included in the meeting. If the total port capacity for the organization exceeds the Max Ports value (for all meetings that are scheduled in the time slot), the system rejects the attempt to schedule this meeting. You may choose to bypass organization bandwidth management entirely by always specifying 0 (in the administration console) or null (in API calls) for the endpoint bandwidth, effectively disabling the feature.

Note Rendezvous meetings, which cannot have endpoint participants added at scheduling time, do not affect the bandwidth calculation for an organization.

For more details on organization bandwidth, see the "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection" appendix.

Call Routing

To route calls, the Cisco TelePresence Exchange System first needs to identify the organization or remote service provider for which the call is intended. The system can identify a destination organization if the dial pattern of the call exactly matches the number of a provisioned endpoint. If the dial pattern does not match the number of a provisioned endpoint, the system systematically tries to match the dial pattern of the call with the dial patterns configured on the system for remote service providers and then organizations. If a match is found, the system identifies the associated organization or remote service provider as the destination for the call. If no match is found, the system sends the call to a default route. If you have not configured an active default route, then the system rejects the call.

After the system identifies the destination organization or remote service provider, the system finds the first active route associated with the destination for the call. The route provides a pointer to a resource. The system then forwards the call to the resource associated with the active route. The route also provides a unique tag value that is added to the outgoing SIP message.

In most cases, the resource associated with the active route is a Session Border Controller (SBC). When configured properly, each adjacency on the SBC is also assigned a unique tag value. When the SBC receives a SIP message from the Cisco TelePresence Exchange System, the SBC routes the call to the adjacency whose tag matches the tag on the message.

Dial Patterns

For direct dial and SIP dial out calls, the Cisco TelePresence Exchange System provides call routing capabilities that are based on matching (specifying and recognizing) strings of text called dial patterns. You can specify the rule for dial pattern matching to be based on either a number or domain (the characters that follow the @ symbol in the SIP URI) and then associate the rule to a destination organization or remote service provider.

If the dial pattern rule is specified for a destination number, you can further configure the dial pattern rule to exactly match the dial pattern of the destination number or to match only the prefix, suffix, or regular expression of the destination number. If the dial pattern rule is specified for a destination domain,

you can only configure the dial pattern rule to exactly match the characters that follow the @ symbol in the SIP URI.

Inter/Intra-Service Provider Policy Engine and Whitelist Groups

The policy engine enables you to define policies that control incoming and outgoing calls between service providers (also known as inter-service provider calls) or between organizations associated with a single service provider (also known as intra-service provider calls). The policies apply to provisioned and unprovisioned endpoints. The Cisco TelePresence Exchange System call detail records (CDRs) identify calls that are rejected due to policy restriction.

For calls from one service provider to another, a flag at the organization level enables you to allow or deny outgoing calls to other service providers. (This includes Meet-Me, Rendezvous, and direct-dial calls, because the Cisco TelePresence Exchange System cannot determine the type of an outgoing call.) Two additional flags at the organization level enable you to allow or deny incoming direct-dial calls from another service provider and to allow or deny incoming Meet-Me and Rendezvous calls from another service provider.

For calls within a single service provider, you can define whitelist groups that determine which organizations can dial each other directly. (Meet-Me and Rendezvous meeting calls are always allowed between organizations that belong to the same service provider.) A whitelist group can contain more than one organization, and an organization can belong to more than one whitelist group.

CHAPTER 2

Overview of the Administration Console

The administration console provides a graphical user interface to configure, monitor, and troubleshoot the Cisco TelePresence Exchange System product. The following sections provide a general description of the administration console:

Accessing the Administration Console

You can access the administration console from any computer that can connect to the virtual IP (VIP) address of the outside VLAN interface on the Cisco Application Control Engine (ACE) that is associated with this Cisco TelePresence Exchange System.

Procedure

To access the administration console, do the following procedure:

Step 1 Browse to http://<*IP address of the administration server*>:8080/ctxadmin.

In some configurations, you do not need to specify the 8080 port value.

Step 2 To log in to the system, enter the following default username and password, and then press **Return**.

username: **admin**

password: **cisco**

Note For security reasons, Cisco recommends that you change the password of the default user. For instructions, see the "Editing User Settings" section on page 8-5.

Screen Layout

The administration console user interface includes a banner pane, a navigation pane, system status, and a content area. These elements are described in the following topics:

Banner Pane

The banner pane, which is displayed at the top of all administration console windows, lists the name of the software application and provides the following functions:

- **Message display**—Shows important messages regarding the administration console status.
- **User**—Shows the name of the user that is currently logged in to the administration console. Click the name to show details about the user.

  From the user details window that opens, you can also view a listing of other users on the system as well as edit your own settings by clicking the appropriate button. As a system administrator, you can modify details for all users.
- **Log Out**—Click to log out of the system.
- **About**—Click to show the software version and licensing information.
- **Upgrade**—Click to show the Cisco TelePresence Exchange System Upgrade window. Enter the default username and password; then, click **LOG IN**.
- **Help**—Click to show online help for the administration console.

Navigation Pane

The navigation pane is on the left side of the administration console. The navigation pane lists items by category that you can view and configure.

When you click a category, the menu expands to show the items in that category. Table 2-1 describes the categories of the navigation pane.

Table 2-1 Navigation Categories

Category	Description
System	Basic system settings. Also shows information about system status.
Media Resources	Configuring Cisco TelePresence Multipoint Switch resources, IVR resources, SIP resources, Cisco Unified Communications Manager (Unified CM) resources, Cisco TelePresence Server MSE 8710 resources, and Cisco TelePresence MCU MSE 8510 resources.
Customers	Configuring service providers, regions, and organizations. You can also configure resource groups and whitelist groups.

Table 2-1 Navigation Categories (continued)

Category	Description
Endpoint Management	Configuring endpoints, media profiles, and Cisco TelePresence Manager resources.
Call Routing	Configuring dial plans, call routing, remote service providers, and call detail records (CDRs).
Collaboration Services	Configuring meetings, service numbers, and IVR prompts. You can also configure active meetings and reservation types.
Licensing	Managing licenses.
Diagnostics	Viewing meeting diagnostics and event audit trails. You can also view reservation pool and allocation pool usage.

System Status

The system status appears below the navigation pane and provides a status summary of scheduling, attending, One-Button-to-Push (OBTP), and system configuration on the Cisco TelePresence Exchange System. For additional information about system status, see the "Understanding System Status" section on page 8-1.

Content Area

The main content area appears to the right of the navigation pane. When you click a menu item in the navigation pane, the content that is associated with that item shows in the content area. The content shows as an item table, which lists the currently configured items.

Usage Guidelines

Be aware of the following usage guidelines when you perform tasks in the administration console:

- Administration Console Timeout—For system security, the administration console session times out when the user is inactive for 30 minutes. The current administration console window remains open. When the user attempts to perform a new function, the administration console prompts the user to reenter login information.
  - To log in again, enter your username and password, and then click **Log In**.
  - To exit the administration console, click **Log Out** (located in the top-right corner of the administration console banner pane).
- The administration console supports the following browsers:
  - Microsoft Internet Explorer (IE) versions 8.x and 9.x
  - Mozilla Firefox versions 3.7 and later
- You can simultaneously run multiple browser sessions on different machines.
- You cannot run multiple sessions within the same browser on a single machine. However, you can open multiple browsers (with one session per browser).

- In order to play IVR prompts in the administration console, the browser requires a media player plug-in capable of playing the .au audio file format.
- In the event of a database failure, the administration console may take up to two minutes to respond after database failover.

Media Resource Operational States

The Cisco TelePresence Exchange System call engine monitors the operational state of the SBC and the Cisco TelePresence Multipoint Switch systems that are installed in the network by conducting regular polling of these systems at two minute intervals. You can also monitor the following bridge types:

- Cisco TelePresence Multipoint Switch (CTMS)
- Cisco TelePresence Server MSE 8710 (TPS)
- Cisco TelePresence MSE 8000 Series
- Cisco TelePresence Manager (CTS-Manager)

You can view the operational state from the administration console. The operational states are defined as follows:

- **Online**—Indicates that the system responds to polling from the Cisco TelePresence Exchange System.
- **Offline**—Indicates that the system is not responding to polling. If the system subsequently recovers and starts responding to the polling, the Cisco TelePresence Exchange System sets the operational state to online after receiving three consecutive responses. The Cisco TelePresence Exchange System continues to poll an offline system until it receives a response.
- **Maintenance**—Indicates that the system is not available. The system administrator must manually set the state to maintenance. The Cisco TelePresence Exchange System does not poll systems in maintenance state.

Note To return a system to an active state from an maintenance state, you must manually disable the maintenance state, so that the Cisco TelePresence Exchange System starts to poll the system again. When the system responds to polling, it is reset to an online state.

Common Field Properties

Table 2-2 describes the field properties for fields that are commonly used in the administration console.

Table 2-2 Common Field Properties

Field Name	Description
Name	No limit on the number of characters. Special characters and spaces can be used after the first character, which must be alphanumeric.
Description	Maximum of 255 characters. Special characters and spaces can be used after the first character, which must be alphanumeric.

Table 2-2 Common Field Properties (continued)

Field Name	Description
Node Name	Maximum of 128 characters. Special characters and spaces can be used after the first character, which must be alphanumeric.
IP Address	IPv4 address entered in dotted decimal notation (xxx.xxx.xxx.xxx), where xxx is a value between 0 and 255 with no leading zeros.

Sorting and Filtering Lists in the Administration Console

To	Do This
Sort a list.	1. Click the relevant column header to sort the list in ascending alphanumeric order. 2. Click the column header again to sort the list in descending alphanumeric order.
Filter a list.	1. Click the T icon in the relevant column header. 2. Enter the text string or select the conditions against which you want to find matches. If you see two text fields for a time-related column, then you can specify a range of times for the filter by entering the start date or time and the end date or time. These time-related fields accept a wide range of inputs, such as “yesterday” or “8/5/12” or “10:30 AM”. 3. Click **Filter**.
Clear filters for a single column.	1. Click the **T** icon in the relevant column header. 2. Click **Clear**.
Clear all filters for a list.	1. Scroll to the bottom of the list. 2. Click **Clear Filters**.

CHAPTER 3

Overview of the CLI

As part of the installation process, you use the command line interface (CLI) to synchronize the database servers. Although you complete most of the configuration tasks via the administration console, the CLI enables you to complete some optional tasks, such as configuring SNMP, configuring CDP, or changing the IP addresses of certain servers. You can also use the CLI to show and change the network configurations, check the status of or restart a service, restart a server, or troubleshoot the system.

This chapter includes the following sections:

Accessing the CLI

Use one of the following methods to access the CLI on any of the Cisco TelePresence Exchange System servers:

- Access the CLI via the console.

  If you need to change the IP address of the server, Cisco recommends that you use the console connection to avoid losing connectivity to the server.

- Access the CLI via SSH.

  You need a remote connection with a terminal emulation program, such as the Windows SSH client, to log in to the CLI remotely via SSH.

Whether you use the console or SSH, enter the Administrator Login username and password to log in to the CLI. The administrator username and password are specified during the installation. See the set password admin command reference for information about changing the administrator password.

Related Topics

- Command Reference
- Password Recovery

Getting Help for the CLI

Use one of the following methods to find help for the CLI on any of the Cisco TelePresence Exchange System servers:

- At any time, you can enter a question mark (**?**) to see a list of entry options. For example:

```
admin: utils service ?
       utils service adminserver*
       utils service corosync*
       utils service crm*
       utils service database*
       utils service nodemanager*
       utils service sipserver*
```

- For help with a specific command, enter **help** followed by the command name. For example:

```
admin: help utils service crm

      utils service crm status

Example:
admin: utils service crm status
============
Last updated: Tue Jul 19 22:53:47 2011
Stack: openais
Current DC: ctx-host1-1 - partition with quorum
Version: 1.0.9-89bd754939df5150de7cd76835f98fe90851b677
6 Nodes configured, 6 expected votes
4 Resources configured.
============

Online: [ ctx-host-1 ctx-host-2 ctx-host-3 ctx-host-4 ctx-host-5 ctx-host-6 ]

 Resource Group: mysql
     fs_mysql   (ocf::heartbeat:Filesystem):    Started ctx-host-1
     ip_mysql   (ocf::heartbeat:IPaddr2):       Started ctx-host-2
     mysqld     (ocf::heartbeat:mysql): Started ctx-host-1
 Master/Slave Set: ms_drbd_mysql
     Masters: [ ctx-host-1 ]
     Slaves: [ ctx-host-2 ]
 Clone Set: stonith-clone
     Started: [ ctx-host-1 ctx-host-2 ]
 Clone Set: pingclone
     Started: [ ctx-host-1 ctx-host-2 ]
```

- For details about each command, see Appendix C, “Command Reference.”

PART 2

Installing the Cisco TelePresence Exchange System

CHAPTER 4

Preparing for Installation

Revised July 3, 2012

The following sections describe the activities that you must complete before installing the Cisco TelePresence Exchange System software:

Preinstallation Checklist

Preinstallation Tasks	Checkoff
Rack mount the Cisco TelePresence Exchange System and solution components. See the "Recommendations for Rack Mounting the Cisco TelePresence Exchange System and Other Solution Components" section on page 4-2.	
Check that the power cords for your servers and monitors are securely attached and plugged in to working power sources. We recommend that you use an uninterruptible power supply (UPS) or dual power sources, especially for the database servers.	
Check that the servers are properly cabled. See the "Cabling Requirements" section on page 4-2.	
Check that you can access the Cisco TelePresence Exchange System servers (database, administration, and call engine) by using a local console.	
Verify that your Cisco TelePresence Exchange System installation DVD has the latest software version. If you are not sure, or if you do not have the DVD, download the latest software from the following URL, and burn the disk image onto a DVD: http://www.cisco.com/go/ctx-download.	

Preinstallation Tasks	Checkoff
Verify that you have all the required information before you begin the installation. See the "Gathering Required Information Before Installation" section on page 4-5.	
If you plan to enable the domain name system (DNS) client on each Cisco TelePresence Exchange System server, enter each hostname and IP address into the DNS servers, including the virtual hostname and virtual IP (VIP) address that are shared by the database servers.	
Verify that each VLAN that will have a Cisco TelePresence Exchange System server can connect to the NTP servers.	
(Optional) Set up the IMM for each server to enable remote control of each server. See the "Setting Up the IMM" section on page 4-7.	

Recommendations for Rack Mounting the Cisco TelePresence Exchange System and Other Solution Components

Note Leave a space of one-third of a rack unit (RU) between each unit to provide proper ventilation.

Use the following list to determine the rack position of each solution component, where item 1 is at the top of the rack:

1. Cisco router with interactive voice response (IVR)—two systems
2. Cisco Application Control Engine (ACE)—two systems
3. Cisco TelePresence Video Communication Server
4. Cisco TelePresence Manager
5. Cisco TelePresence Multipoint Switch
6. Keyboard-video-mouse (KVM) switch for console access to all systems
7. Power distribution unit (PDU)—two units for redundancy
8. Cisco Catalyst Switch—two systems
9. Cisco TelePresence Exchange System database servers—two servers
10. Cisco TelePresence Exchange System administration servers—two servers
11. Cisco TelePresence Exchange System call engine servers—two servers

Note The Cisco Unified Communications Manager and Cisco Session Border Controller are also part of the Cisco TelePresence Exchange System solution, but Cisco expects that those components are already installed and in use in the network and therefore does not provide rack-mounting recommendations.

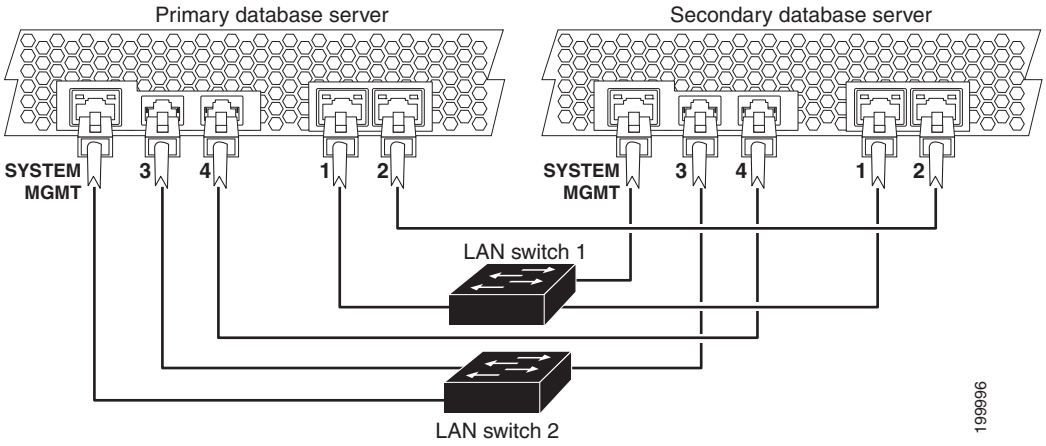
Cabling Requirements

Cabling Requirements for the Database Servers

To provide active/standby redundancy for the database servers, you must connect the primary and secondary database servers as shown in Figure 4-1.

Note You can use straight-through or crossover cables for these connections.

Figure 4-1 Required Cabling Between the Database Servers



Port label	Interface	Bonded Interface
1	Ethernet 0—application data and heartbeat	Bond 0
2	Ethernet 1—data replication between database servers	Bond 1
3	Ethernet 2—application data and heartbeat	Bond 0
4	Ethernet 3—data replication between database servers	Bond 1
SYSTEM MGMT (optional)	Integrated management module (IMM) You are not required to use the IMM interface, which enables remote control of the server.	—

When the servers are cabled as shown in Figure 4-1, the system remains connected if any one component or cable fails. Specifically:

- The NICs on each server are connected to separate switches.

  In each server, Ethernet 0 and Ethernet 1 are on one NIC, while Ethernet 2 and Ethernet 3 are on a second NIC.
- On each database server, the Cisco TelePresence Exchange System software automatically implements NIC teaming to bond the following interfaces together:
  - Ethernet 0 with Ethernet 2.
  - Ethernet 1 with Ethernet 3.
- Each NIC has a heartbeat connection to the redundant server.
- You are not required to use the IMM interfaces, but if you do, then we recommend that you cable them as shown in Figure 4-1 to connect the IMM interfaces to separate switches.

Related Topics

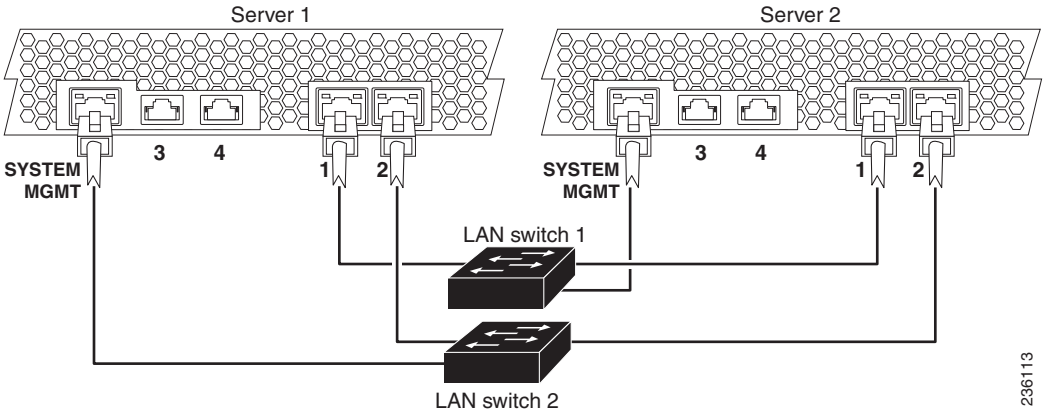
- Setting Up the IMM, page 4-7

Cabling Requirements for the Administration and Call Engine Servers

To provide switch and network redundancy for the administration servers and call engine servers, you must connect the servers as shown in Figure 4-2.

Note You can use straight-through or crossover cables for these connections.

Figure 4-2 Required Cabling Between Administration Servers and Between Call Engine Servers



Port label	Interface	Bonded Interface
1	Ethernet 0—data	Bond 0
2	Ethernet 1—data	Bond 0
3	Ethernet 2—currently not used	—
4	Ethernet 3—currently not used	—
SYSTEM MGMT (optional)	Integrated management module (IMM) You are not required to use the IMM interface, which enables remote control of the server.	—

On each administration server and call engine server, the Cisco TelePresence Exchange System software bonds Ethernet 0 with Ethernet 1. When the servers are cabled as shown in Figure 4-2, the bonded interface is connected to both LAN switches.

You are not required to use the IMM interfaces, but if you do, then we recommend that you connect the IMM interfaces to separate LAN switches.

VLAN Requirements and Restrictions

Apply the following requirements, restrictions, and recommendations as you assign IP addresses to the Cisco TelePresence Exchange System:

- You cannot assign any IP addresses in the 10.0.0.*x*/8 address space.
- The data network interfaces of all nodes in the Cisco TelePresence Exchange System server cluster must be on the same VLAN. Therefore, the same VLAN must be used for all of the following interfaces:
  - Ethernet 0 and Ethernet 2 of both database servers.
  - Ethernet 0 and Ethernet 1 of both administration servers and both call engine servers.

Note This VLAN is the inside network VLAN that you will configure on the Cisco Application Control Engine (ACE) in a redundant or non-redundant ACE configuration.

- The data VLAN of the Cisco TelePresence Exchange System must be separate from the data VLANs that are used by the following solution components:
  - Cisco Unified Communications Manager
  - Cisco Session Border Controller
  - Cisco TelePresence Multipoint Switch
  - Cisco Router with Integrated Voice Response (IVR)
- You must be able to ping the default gateway from each of the Cisco TelePresence Exchange System servers.
- If you use the integrated management module (IMM) interfaces on the Cisco TelePresence Exchange System servers, we recommend that you use a separate system management VLAN for the IMM interfaces.

Note Make sure that packets can be routed between all of the VLANs that you implement for the Cisco TelePresence Exchange System solution.

Gathering Required Information Before Installation

Complete the worksheets in Appendix A, "Installation Worksheets," as you collect the following information. Before you proceed, however, read the "VLAN Requirements and Restrictions" section on page 4-5.

- Unique hostnames:
  - One hostname for each of the database, call engine, and administration servers.
  - One virtual hostname to be shared by the two database servers.
- Unique IP addresses and their subnet masks:
  - One IP address for each of the database, call engine, and administration servers.
  - One virtual IP (VIP) address to be shared by the two database servers. The database VIP is the only address that the network recognizes for the database servers, only one of which is active at any given time.

  - (Optional) One IP address for each integrated management module (IMM) interface. The IMMs enable remote control of the servers.
- IP addresses of the default gateways:
  - IP address of the default gateway for the data network interfaces. (This address is the IP address of the inside network interface VLAN of the Cisco Application Control Engine.)
  - (Optional) IP address of the default gateway for the IMM interfaces.
- Administrator usernames and passwords:
  - For accessing the CLI of each database, administration, and call engine server. You must use the same administrator username and password on all Cisco TelePresence Exchange System servers, because the administration servers also use the administrator credentials over SSH to get the status of all nodes in the server cluster.
  - (Optional) For accessing each IMM interface, which enables remote control of the server.
- A security password.

  The database server uses this password to authenticate data requests from the administration and call engine servers. Therefore, you must define the same security password for the database, administration, and call engine servers.

  Note After you configure the security password on a server, you cannot change it without reinstalling the server.

- (Optional) Domain Name System (DNS) information:
  - IP address of a primary DNS server.
  - (Optional) IP address of a secondary DNS server.
  - Domain name.
- IP addresses, hostnames, or pool names for external Network Time Protocol (NTP) clocking sources. Cisco recommends that you use at least three external NTP clocking sources.

  You must configure the same NTP entries on the database, call engine, and administration servers.
- For the SIP load balancer, which is the Cisco Application Control Engine (ACE):
  - VIP address.
  - Port number—Cisco recommends that you use the default port 5060.
- For generating locally significant certificates (LSC) for each database, call engine, and administration server:
  - Organization—typically your company name.
  - Unit—typically your business unit and department.
  - Location—typically the building, floor, and rack in which the server is installed.
  - State and Country—where the server is located.

  Use the following guidelines to determine each entry for generating LSCs:
  - Refer to your company guidelines for format and entry requirements.
  - Supported characters include alphanumeric, space, and the following special characters: .,-_:;{}()[]#.
  - Each field supports up to 255 characters.

Setting Up the IMM

You may choose to set up the IMM on each Cisco TelePresence Exchange System server to enable you to control each server remotely; this remote access is available whenever the server is plugged in to a working power source, even if the server is turned off.

To set up the IMM, complete the following tasks:

- Setting Up the IMM Network Connection, page 4-7
- Creating an IMM User Account, page 4-8
- Enabling SSH for the IMM, page 4-9

Setting Up the IMM Network Connection

Before You Begin

Find your completed Appendix A, "Installation Worksheets."

Procedure

Step 1 Attach a console to the console port of the server.

The console port is located on the front of the server.

Step 2 Turn the server on by pressing the power button that is located on the front of the server.

After approximately one minute, an IBM System x screen is displayed on the console.

Step 3 Watch for the **F1 <setup>** option to appear at the bottom of the IBM System x screen. This may take another minute or two.

Step 4 Press the **F1** key as soon as the option appears.

If the option disappears before you press F1, then turn the server off and on, and try again.

Tip At any time in the following steps, if you accidentally end up in the wrong screen or select the wrong field, press the **Esc** key to back out of that screen or field selection.

Step 5 In the System Configuration and Boot Management screen, select **System Settings**.

Step 6 In the System Settings screen, select **Integrated Management Module**.

Step 7 In the Integrated Management Module screen, select **Network Configuration**.

Step 8 In the Network Configuration screen, select the **DHCP Control** field value.

Step 9 In the DHCP Control field, select the **Static IP** option.

Step 10 Enter the IP address, subnet mask, and default gateway IP address for the IMM interface.

Step 11 Select **Save Network Settings**.

Step 12 Press the **Enter** or **Return** key to continue.

Step 13 Press the **Esc** key repeatedly to exit each setup screen.

Step 14 When prompted, press the **Y** key to exit the setup utility.

The server reboots.

Step 15 Repeat this procedure for the redundant server.

What to Do Next

Proceed to the "Creating an IMM User Account" section on page 4-8.

Creating an IMM User Account

Before You Begin

- Complete the procedure in the "Setting Up the IMM Network Connection" section on page 4-7.
- Complete this task by using one of the following web browsers:
  - Microsoft Internet Explorer version 6.0 or later with the latest Service Pack
  - Mozilla Firefox version 1.5 or later
- Make sure that the browser allows popup windows from the IMM.

Procedure

Step 1 Point a web browser to the IP address of the IMM interface.

Step 2 Log in to the IMM web interface with following default username and password:

username: **USERID**

password: **PASSW0RD** (Enter a zero instead of the letter O.)

Step 3 (Optional) Set the inactive session timeout value.

Step 4 Click **Continue**.

Step 5 In the left navigation area, select **System > IMM Control > Login Profiles**.

Step 6 In the Login Profiles area, click **Add User**.

Step 7 In the **Login ID** field, enter the username.

The username must have between 4 and 16 characters, and may include uppercase and lowercase letters, numbers, periods, and underscores.

Step 8 In the **Password** and **Confirm password** fields, enter a password that contains a minimum of five characters, one of which must be a nonalphabetic character. You cannot use a null or empty password.

Step 9 Select the **Supervisor** authority level, which provides unlimited access.

Step 10 Click **Save**.

Step 11 (Optional) To prevent unauthorized access, change the password for the default IMM user account by completing these steps:

a. In the Login Profiles area, click the **USERID** Login ID.

b. Enter a new password into the **Password** and **Confirm password** fields.

c. Click **Save**.

What to Do Next

Proceed to the "Enabling SSH for the IMM" section on page 4-9.

Enabling SSH for the IMM

The secure shell (SSH) provides secure access to the command-line interface (CLI) and the serial redirect features of the IMM. An SSH user is authenticated by exchanging the username and password, which are sent after the encryption channel is established. The username and password can be one of the 12 username and password pairs that the server stores locally, or they can be stored on a lightweight directory access protocol (LDAP) server. Public key authentication is not supported.

Before You Begin

- Complete the procedure in the "Creating an IMM User Account" section on page 4-8.
- Complete this task by using one of the following web browsers:
  - Microsoft Internet Explorer version 6.0 or later with the latest Service Pack
  - Mozilla Firefox version 1.5 or later
- Make sure that the browser allows popup windows from the IMM.

Procedure

Step 1 In the IMM web interface, choose **System > IMM Control > Security**.

Step 2 Scroll down to the **SSH Server Key Management** area.

Step 3 Click **Generate SSH Server Private Key**.

An SSH server key is used to authenticate the identity of the SSH server to the client.

Step 4 Wait for the progress bar to indicate completion.

Step 5 In the **SSH Server** field, select **Enabled**.

Step 6 Click **Save**.

Step 7 In the left navigation area, select **System > IMM Control > Restart IMM**.

Step 8 Click **Restart**.

Step 9 Click **OK** to confirm the restart.

APPENDIX 5

Installing the Software

This chapter describes how to install the software for the Cisco TelePresence Exchange System.

Determining the Method and Order of Installation

You can install the servers in series or in parallel. To determine which method is best for you, see Table 5-1 and the following sections:

Table 5-1 Comparison of Serial and Parallel Cisco TelePresence Exchange System Installation

Installation Method	Advantage	Disadvantage
Serial	Less opportunity for entry errors. You enter information into the installation wizard for only one server at a time.	Longer installation process. Each server installation requires 40 minutes to install.[1] So the full serial installation requires 240 minutes (6 servers × 40 minutes each).
Parallel	Shorter installation process. Each server pair requires 40 minutes to install.[1] You must install the database servers serially before you begin to install the administration and call engine servers. If you install all four of the administration and call engine servers at the same time, the full parallel installation requires 160 minutes (2 database server installations x 40 minutes each plus 2 parallel installations x 40 minutes).	Greater opportunity for entry errors. You enter information into the installation wizard for two to four servers at a time.

1. If you are installing the Cisco TelePresence Exchange System software on a server that requires a firmware update, the installer automatically begins the update, which typically takes about 30 minutes, before performing the server installation. This time is not included in these estimations.

Serial Installation

Software installation for each server requires approximately 40 minutes when you employ a serial installation. To ensure the proper exchange of information among the Cisco TelePresence Exchange System servers during a serial installation, install the servers in the following order:

1. Install the primary database server.
2. Install the secondary database server.
3. Install the administration and call engine servers. The order in which you install these remaining nodes does not matter.

See the following sections for detailed installation instructions for each server:

- Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers, page 5-4
- Installing the Cisco TelePresence Exchange System Call Engine Servers, page 5-9
- Installing the Cisco TelePresence Exchange System Administration Servers, page 5-14

Parallel Installation

Note You need one copy of the installation DVD for each server that you plan to install in parallel.

To reduce the overall installation time of the Cisco TelePresence Exchange System servers, you can install some of the servers in parallel in the following order:

1. Install the primary database server.
2. When the primary database server installation is complete, install the secondary database server.

   Ensure that the database server installations and synchronization are complete before you proceed to install the call engine and administration servers.
3. Install the administration and call engine servers in parallel. You can start the installation for as many servers as you have installation DVDs.

See the following sections for detailed installation instructions for each server:

- Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers, page 5-4
- Installing the Cisco TelePresence Exchange System Call Engine Servers, page 5-9
- Installing the Cisco TelePresence Exchange System Administration Servers, page 5-14

Options for Connecting to the Cisco TelePresence Exchange System Servers for Installation

You have two connection options for running the Cisco TelePresence Exchange System installer on each server:

- Direct connection to the console, for example, through a keyboard-video-mouse (KVM) switch.
- Remote connection by using the integrated management module (IMM) interface. See the "Using the IMM to Remotely Install the Cisco TelePresence Exchange System Software" section on page 5-3.

Note Although you may use the IMM to remotely run the installer, the Cisco TelePresence Exchange System installation DVD must be inserted into the server. Cisco currently does not support full remote installation by mounting the DVD or image file using the IMM.

Using the IMM to Remotely Install the Cisco TelePresence Exchange System Software

Before You Begin

- For each server that you want to access remotely, you must first complete the procedures in the "Setting Up the IMM" section on page 4-7.
- Insert the Cisco TelePresence Exchange System installation DVD into the server. Cisco currently does not support full remote installation by mounting the DVD or image file using the IMM.
- Complete this task by using one of the following web browsers:
  - Microsoft Internet Explorer version 8.x or 9.x with the latest Service Pack
  - Mozilla Firefox version 3.7 or later
- Make sure that the web browser allows popup windows from the IMM.

Procedure

Step 1 Point your web browser to the IP address of the IMM interface.

Step 2 Log in to the IMM web interface.

Step 3 Select **Continue**.

Step 4 Select **System > Tasks > Remote Control**.

Step 5 Click **Start Remote Control in Single User Mode**.

This opens a console window, which you will use later to enter information as the installer runs.

Tip If the console window does not open, press and hold down the Control key and click **Start Remote Control in Single User Mode** again. Continue to hold the Control key until the window opens.

Step 6 In the IMM web interface, select **System > Tasks > Power/Restart**.

Step 7 Click **Restart the Server Immediately**.

Step 8 Click **OK** to confirm the restart.

When the DVD is recognized after the restart, the installer begins to run. Use the console window to complete the installation procedures.

What to Do Next

Complete the installation procedures for the server:

- Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers, page 5-4
- Installing the Cisco TelePresence Exchange System Call Engine Servers, page 5-9
- Installing the Cisco TelePresence Exchange System Administration Servers, page 5-14

Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers

Complete the following tasks in the order shown:

- Installing the Database Server Software, page 5-4
- Checking the Initial High-Availability Roles of the Database Servers, page 5-7
- Checking the Network Connectivity of the Database Servers, page 5-9

Installing the Database Server Software

Complete this task to install the Cisco TelePresence Exchange System database server software onto the server.

Before You Begin

- Complete the tasks and requirements in Chapter 4, "Preparing for Installation."
- Find your completed Appendix A, "Installation Worksheets."
- Choose your installation method. See the "Determining the Method and Order of Installation" section on page 5-1.
- Insert the Cisco TelePresence Exchange System installation DVD into the server.
- Turn on or restart the server. If you are performing the installation remotely via the IMM, complete the procedure in the "Using the IMM to Remotely Install the Cisco TelePresence Exchange System Software" section on page 5-3.

  After the restart, the server recognizes the DVD and automatically runs the installer.

Note If you are installing the Cisco TelePresence Exchange System software on a server that requires a firmware update, the installer automatically begins the update. During the update, the system will restart approximately four times. The update typically takes about 30 minutes. If you are installing by using the IMM, you will temporarily lose connectivity during the firmware update.

Tip To move among the options in an installer screen, press the **Tab** key. To select a highlighted option, press the **Spacebar**, **Return**, or **Enter** key.

Procedure

Step 1 When the installer prompts you to do a media check of the DVD, take one of the following actions:

- If you previously performed a media check of the installation DVD, select **No**.
- Otherwise, Cisco recommends that you select **Yes**. After the DVD passes the media check, select **OK**.

  If the installation DVD fails the media check, burn a new DVD. Download the software from http://www.cisco.com/go/ctx-download.

After several minutes, the installer displays the current software version that is installed on the server (if any) and the software version on the DVD.

Step 2 In the Proceed with Install screen, select **Yes**.

Step 3 In the Platform Installation Wizard screen, select one of the following options, depending on whether you want to enter the server information before or after the installer spends approximately 30 minutes installing the software on the server:

- To first enter the server information and then install the software, select **Proceed**.
- To first install the software and then enter the server information, select **Skip**.

  If you choose Skip, then after approximately 30 minutes of installing software on the server, take the following actions:

  – The system displays the Pre-existing Configuration Information screen, on which you select **Continue**. Pre-existing configurations are currently not supported.

  – The system then returns to the Platform Installation Wizard screen, on which you select **Proceed**.

Step 4 At the Node Role Configuration screen, enter **database** as the role of the node, then select **OK**.

Step 5 Verify that the confirmation screen indicates that this node will be configured to run the **database**. If correct, select **Proceed**.

Note If a different server installation screen appears, select **Back** to return to Step 4.

Step 6 In the Static Network Configuration screen, complete the following steps:

Note If you are using the serial installation method, always install the primary (active) database server before you install the secondary (backup) database server.

a. Enter the host name, IP address, and subnet mask for the database server.

b. Enter the IP address for the default gateway.

c. Verify your entries and select **OK**.

Step 7 In the DNS Client Configuration screen, select **No**. The Domain Name Server (DNS) client is not supported on the database server.

Step 8 In the Database Redundancy Configuration screens, complete the following steps:

a. When prompted to enable redundancy on the database node, select **Yes**.

b. When asked whether to configure this node as the *primary* database server, select **Yes** or **No**, depending on which database server you are installing (**Yes** for primary, **No** for secondary).

c. Enter the VIP address to be shared by the primary and secondary database servers.

d. Enter the hostname and IP address for the *peer* server:

- If you are configuring the primary database server, then enter details for the secondary server.
- If you are configuring the secondary database server, then enter details for the primary server.

e. Select **OK**.

Step 9 In the Administrator Login Configuration screen, complete the following steps to create a Linux account for accessing the CLI of the database server:

Note You must use the same administrator username and password for all database, administration, and call engine servers in the cluster.

a. In the Administrator ID field, enter a username.

b. In the Password and Confirm Password fields, enter a password.

c. Select **OK**.

Step 10 In the Certificate Information screen, complete the following steps to generate a locally significant certificate (LSC) for the server:

Note Refer to your company guidelines on the format for each of these entries.

a. In the Organization field, enter your company name.

b. In the Unit field, enter descriptive information about the server.

Example: *business-unit*, *department*

c. Enter the location of the server.

Example: *building-name*, *floor*, *rack*

d. Enter the state in which the server is located.

You can enter an abbreviation or the full name for the state.

e. Select the country in which the server is located.

Enter the first letter of the country name, and use the up and down arrows to select the country. Then press the **Tab** key.

f. Select **OK**.

Step 11 In the Network Time Protocol Client Configuration screen, complete these steps:

a. Enter at least one NTP server IP address, hostname, or pool name.

Cisco recommends that you configure at least three external NTP entries.

Note You must use the same NTP entries on all database, call engine, and administration servers.

b. Take one of the following actions, the availability of which depends on whether you chose to enter the server information before or after installing the software in Step 3:

- Select **Test** to confirm connectivity to the NTP entries, and then select **Proceed**.
- Select **OK**.

Step 12 In the Security Configuration screen, enter the security password, confirm the password, and select **OK**.

Note You must configure the same security password on all database, administration, and call engine servers. After you configure the security password on a server, you cannot change it without reinstalling the server.

Caution This is your last chance in the installation wizard to select **Back** to verify your entries. Complete the next step only when you are sure that the entries that you made throughout this procedure are correct.

Step 13 In the Platform Configuration Confirmation screen, click **OK**.

If, in Step 3, you chose to proceed to enter the server information before installing the software, the following information applies:

- The installer spends approximately 30 minutes installing the software.
- If the system has problems with the information that you entered in the installation wizard, you will be prompted to correct the information.

The server ejects the installation DVD and reboots the server while completing the installation. This process takes approximately 10 minutes. When complete, the system prompts you to log in to the CLI.

```
The installation of Cisco TelePresence Exchange System has completed successfully.

Cisco TelePresence Exchange System x.x.x.x
hostname login:
```

What To Do Next

If you have not yet installed the software for the secondary database server, do so now by repeating this procedure.

Otherwise, proceed to the "Checking the Initial High-Availability Roles of the Database Servers" section on page 5-7.

Checking the Initial High-Availability Roles of the Database Servers

After the secondary database server is installed, the database servers should automatically begin to synchronize with each other. Complete this task on each database server to confirm the correct initial high-availability (HA) role of primary or secondary, and to verify that the databases have begun synchronization.

Note The database synchronization process typically takes about 40 minutes to complete. During this time, after you verify that synchronization has begun, you can continue with the installation process.

Procedure

Step 1 Log in to the CLI of the database server.

```
Cisco TelePresence Exchange System x.x.x.x
hostname login: <username>
Password: <password>

Command Line Interface is starting up, please wait...

    Welcome to the Platform Command Line Interface

admin:
```

Step 2 Enter the **utils service database status** command.

The following example shows sample output from a database server that was installed with the primary role:

```
admin: utils service database status
The initial configured HA role of this node      : primary
The current HA role of this node                 : primary
The database vip address                         : 10.22.130.61
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.50
Corosync status                                  : Running PID <19250>
Current Designated Controller (DC)               : ctx-db-1 - partition with quorum
MySQL status                                     : Running pid  15633
Connection Sync Status                           : Connected
Role (this-node/peer-node)                       : Primary/Secondary
Disk Status (this-node/peer-node)                : UpToDate/UpToDate
```

The following example shows sample output from a database server that was installed with the secondary role:

```
admin: utils service database status
The initial configured HA role of this node      : secondary
The current HA role of this node                 : secondary
The database vip address                         : 10.22.130.61
Node name                                        : ctx-db-2
Node IP address                                  : 10.22.130.58
Corosync status                                  : Running PID <26656>
Current Designated Controller (DC)               : ctx-db-1 - partition with quorum
MySQL status                                     : Not running (only runs on database
server with current role primary.)
Connection Sync Status                           : Connected
Role (this-node/peer-node)                       : Secondary/Primary
Disk Status (this-node/peer-node)                : UpToDate/UpToDate
```

Tip While the databases are synchronizing, the Connection Sync Status output displays "SyncTarget <*percentage*>". If you see a Connection Sync Status of "Unconfigured," synchronization did not start successfully. Check the network connectivity between the database servers, and verify that all Cisco TelePresence Exchange System servers are in the same VLAN.

Related Topics

- Appendix C, "Command Reference"

Checking the Network Connectivity of the Database Servers

Enter the following command on each database server to attempt to reach one of the Cisco TelePresence Exchange System solution components in another VLAN, such as the Cisco Unified Communications Manager or the Cisco Session Border Controller:

utils network ping *ip-address*

The output confirms network connectivity:

```
admin: utils network ping 10.68.10.80
PING 10.68.10.80 (10.68.10.80) 56(84) bytes of data.
64 bytes from 10.68.10.80: icmp_seq=0 ttl=247 time=1.38 ms
64 bytes from 10.68.10.80: icmp_seq=1 ttl=247 time=1.39 ms
64 bytes from 10.68.10.80: icmp_seq=2 ttl=247 time=1.42 ms
64 bytes from 10.68.10.80: icmp_seq=3 ttl=247 time=1.63 ms

--- 10.68.10.80 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 1.386/1.461/1.636/0.101 ms, pipe 2
```

Related Topics

- Appendix C, "Command Reference"

Installing the Cisco TelePresence Exchange System Call Engine Servers

Complete the following tasks in the order shown:

- Installing the Call Engine Server Software, page 5-9
- Checking the Call Engine Server Status and Network Connectivity, page 5-13

Installing the Call Engine Server Software

Complete this task to install the Cisco TelePresence Exchange System call engine server software onto the server.

Before You Begin

- Complete the tasks in the "Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers" section on page 5-4.
- Find your completed Appendix A, "Installation Worksheets."
- Insert the Cisco TelePresence Exchange System installation DVD into the server.
- Turn on or restart the server. If you are performing the installation remotely via the IMM, complete the procedure in the "Using the IMM to Remotely Install the Cisco TelePresence Exchange System Software" section on page 5-3.

  After the restart, the server recognizes the DVD and automatically runs the installer.

Note If you are installing the Cisco TelePresence Exchange System software on a server that requires a firmware update, the installer automatically begins the update. During the update, the system will restart approximately four times. The update typically takes about 30 minutes. If you are installing by using the IMM, you will temporarily lose connectivity during the firmware update.

Tip To move among the options in an installer screen, press the **Tab** key. To select a highlighted option, press the **Spacebar**, **Return**, or **Enter** key.

Procedure

Step 1 When the installer prompts you to do a media check of the DVD, take one of the following actions:

- If you have already performed a media check of the installation DVD, select **No**.
- Otherwise, Cisco recommends that you select **Yes**. After the DVD passes the media check, select **OK**.

  If the installation DVD fails the media check, burn a new DVD. Download the software from http://www.cisco.com/go/ctx-download.

After several minutes, the installer displays the current software version that is installed on the server (if any) and the software version on the DVD.

Step 2 In the Proceed with Install screen, select **Yes**.

Step 3 In the Platform Installation Wizard screen, select one of the following options, depending on whether you want to enter the server information before or after the installer spends approximately 30 minutes installing the software on the server:

- To first enter the server information and then install the software, select **Proceed**.
- To first install the software and then enter the server information, select **Skip**.

  If you choose Skip, after approximately 30 minutes of installing software on the server, take the following actions:

  – The system displays the Pre-existing Configuration Information screen, on which you select **Continue**. Pre-existing configurations are currently not supported.

  – The system then returns to the Platform Installation Wizard screen, on which you select **Proceed**.

Step 4 At the Node Role Configuration screen, enter **engine** as the role of the node, then select **OK**.

Step 5 Verify that the confirmation screen indicates that this node will be configured to run the *call processing engine*. If correct, select **Proceed**.

Caution If a different server installation screen appears, select **Back** to return to Step 4.

Step 6 In the Cisco TelePresence Exchange System Other Nodes screen, complete these steps:

a. In the Database node name (Mandatory) field, enter the virtual hostname that is shared by the database servers.

b. In the Database node IP Address (Mandatory) field, enter the virtual IP (VIP) address that is shared by the database servers.

c. Leave the remaining fields blank.

d. Select **OK**.

Step 7 In the Static Network Configuration screen, complete these steps:

a. Enter the host name, IP address, and subnet mask for the call engine server.

b. Enter the IP address for the default gateway.

c. Select **OK**.

Step 8 In the DNS Client Configuration screen, select **No**. The Domain Name Server (DNS) client is not supported on the call engine server.

Step 9 In the SIP Load Balancer Configuration screen, select **Yes**.

Note If you are in the rare situation where you are installing the Cisco TelePresence Exchange System software before you have a functioning Cisco Application Control Engine (ACE) to use as the SIP load balancer, then you may select **No** on the SIP Load Balancer Configuration screen and proceed to Step 11. You must, however, add the SIP load balancer configuration later via the CLI. See the "Configuring SIP Load Balancing on the Call Engine Servers" section on page 28-5.

Step 10 In the SIP Load Balancer Information screen, complete the following steps:

a. IP Address—Enter the VIP address of the ACE.

b. Port—Enter the port number on which the call engine server will connect to the load balancer.

c. Select **OK**.

Step 11 In the Administrator Login Configuration screen, complete the following steps to create a Linux account for accessing the CLI of the call engine server:

Note You must use the same administrator username and password for all database, administration, and call engine servers in the cluster.

a. Enter a username in the Administrator ID field.

b. Enter a password into the Password and Confirm Password fields.

c. Select **OK**.

Step 12 In the Certificate Information screen, complete the following steps to generate a locally significant certificate (LSC) for the server:

Note Refer to your company guidelines on the format for each of these entries.

a. In the Organization field, enter your company name.

b. In the Unit field, enter descriptive information about the server.

Example: *business-unit*, *department*

c. Enter the location of the server.

Example: *building-name*, *floor*, *rack*

d. Enter the state in which the server is located.

You can enter an abbreviation or the full name for the state.

e. Select the country in which the server is located.

Enter the first letter of the country name, and use the up and down arrows to select the country. Then press the **Tab** key.

f. Select **OK**.

Step 13 In the Network Time Protocol Client Configuration screen, complete these steps:

a. Enter the same NTP server IP addresses, hostnames, or pool names that you configured for the database servers.

b. Take one of the following actions, the availability of which depends on whether you chose to enter the server information before or after installing the software in Step 3:

- Select **Test** to confirm connectivity to the NTP entries, and then select **Proceed**.
- Select **OK**.

Step 14 In the Security Configuration screen, enter the security password, confirm the password, and select **OK**.

Note You must configure the same security password on all database, administration, and call engine servers. After you configure the security password on a server, you cannot change it without reinstalling the server.

Caution This is your last chance in the installation wizard to select **Back** to verify your entries. Complete the next step only when you are sure that the entries that you made throughout this procedure are correct.

Step 15 In the Platform Configuration Confirmation screen, select **OK**.

If, in Step 3, you chose to proceed to enter the server information before installing the software, the following information applies:

- The installer spends approximately 30 minutes installing the software.
- If the system has problems with the information that you entered in the installation wizard, you will be prompted to correct the information.

The server ejects the installation DVD and reboots the server while completing the installation. This process takes approximately 10 minutes. When complete, the system prompts you to log in to the CLI.

```
The installation of Cisco TelePresence Exchange System has completed successfully.

Cisco TelePresence Exchange System x.x.x.x
hostname login:
```

What To Do Next

If you have not yet installed the software for the second call engine server, do so now by repeating this procedure.

Otherwise, proceed to the "Checking the Call Engine Server Status and Network Connectivity" section on page 5-13.

Checking the Call Engine Server Status and Network Connectivity

Complete this task to confirm that the call engine server is up and can connect to the other Cisco TelePresence Exchange System servers.

Procedure

Step 1 Log in to the CLI of the call engine server.

```
Cisco TelePresence Exchange System x.x.x.x
hostname login: <username>
Password: <password>

Command Line Interface is starting up, please wait...

    Welcome to the Platform Command Line Interface

admin:
```

Step 2 To verify that the call engine server is running, enter the **utils service sipserver status** command.

In the following example, the call engine server is still starting up. In this case, you would want to wait a few minutes for the server to finish starting up:

```
admin: utils service sipserver status
sipserver.............................Starting - PID <10202>
```

In the following example, the call engine server is up and running:

```
admin: utils service sipserver status
sipserver.............................Running - PID <10202>
```

Step 3 To confirm that the call engine server has network connectivity, enter the following command, specifying the IP or VIP address of any of the Cisco TelePresence Exchange System servers that are already installed:

utils network ping *ip-address*

The output confirms network connectivity:

```
admin: utils network ping 10.22.139.230
PING 10.22.139.230 (10.22.139.230) 56(84) bytes of data.
64 bytes from 10.22.139.230: icmp_seq=0 ttl=64 time=0.512 ms
64 bytes from 10.22.139.230: icmp_seq=1 ttl=64 time=0.093 ms
64 bytes from 10.22.139.230: icmp_seq=2 ttl=64 time=0.090 ms
64 bytes from 10.22.139.230: icmp_seq=3 ttl=64 time=0.090 ms

--- 10.22.139.230 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.090/0.196/0.512/0.182, pipe 2
```

Related Topics

- Appendix C, “Command Reference”

Installing the Cisco TelePresence Exchange System Administration Servers

Complete the following tasks in the order shown:

- Installing the Administration Server Software, page 5-14
- Checking the Administration Server Status and Network Connectivity, page 5-17

Installing the Administration Server Software

Complete this task to install the Cisco TelePresence Exchange System administration server software onto the server.

Before You Begin

- Complete the tasks in the "Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers" section on page 5-4.
- If you are following the serial installation method, also complete the tasks in the "Installing the Cisco TelePresence Exchange System Call Engine Servers" section on page 5-9.
- Find your completed Appendix A, "Installation Worksheets."
- Insert the Cisco TelePresence Exchange System installation DVD into the server.
- Turn on or restart the server. If you are performing the installation remotely via the IMM, complete the procedure in the "Using the IMM to Remotely Install the Cisco TelePresence Exchange System Software" section on page 5-3.

  After the restart, the server recognizes the DVD and automatically runs the installer.

Note If you are installing the Cisco TelePresence Exchange System software on a server that requires a firmware update, the installer automatically begins the update. During the update, the system will restart approximately four times. The update typically takes about 30 minutes. If you are installing by using the IMM, you will temporarily lose connectivity during the firmware update.

Tip To move among the options in an installer screen, press the **Tab** key. To select a highlighted option, press the **Spacebar**, **Return**, or **Enter** key.

Procedure

Step 1 When the installer prompts you to do a media check of the DVD, take one of the following actions:

- If you have already performed a media check of the installation DVD, select **No**.
- Otherwise, Cisco recommends that you select **Yes**. After the DVD passes the media check, select **OK**.

  If the installation DVD fails the media check, burn a new DVD. Download the software from http://www.cisco.com/go/ctx-download.

After several minutes, the installer displays the current software version that is installed on the server (if any) and the software version on the DVD.

Step 2 In the Proceed with Install screen, select **Yes**.

Step 3 In the Platform Installation Wizard screen, select one of the following options, depending on whether you want to enter the server information before or after the installer spends approximately 30 minutes installing the software on the server:

- To first enter the server information and then install the software, select **Proceed**.
- To first install the software and then enter the server information, select **Skip**.

  If you choose Skip, then after approximately 30 minutes of installing software on the server, take the following actions:

  – The system displays the Pre-existing Configuration Information screen, on which you select **Continue**. Pre-existing configurations are currently not supported.

  – The system then returns to the Platform Installation Wizard screen, on which you select **Proceed**.

Step 4 At the Node Role Configuration screen, enter **admin** as the role of the node, then select **OK**.

Step 5 Verify that the confirmation screen indicates that this node will be configured to run the *administration console*. If correct, select **Proceed**.

Caution If a different server installation screen appears, select **Back** to return to Step 4.

Step 6 In the Cisco TelePresence Exchange System Other Nodes screen, complete these steps:

a. In the Database node name (Mandatory) field, enter the virtual hostname that is shared by the database servers.

b. In the Database node IP Address (Mandatory) field, enter the virtual IP (VIP) address that is shared by the database servers.

c. Leave the remaining fields blank.

d. Select **OK**.

Step 7 In the Static Network Configuration screen, complete these steps:

a. Enter the host name, IP address, and subnet mask for the administration server.

b. Enter the IP address for the default gateway.

c. Click **OK**.

Step 8 In the DNS Client Configuration screen, select **No**. The Domain Name Server (DNS) client is not supported on the administration server.

Step 9 In the Administrator Login Configuration screen, complete the following steps to create a Linux account for accessing the CLI of the call engine server:

Note You must use the same administrator username and password for all database, administration, and call engine servers in the cluster.

a. Enter a username in the Administrator ID field.

b. Enter a password into the Password and Confirm Password fields.

c. Select **OK**.

Step 10 In the Certificate Information screen, complete the following steps to generate a locally significant certificate (LSC) for the server:

Note Refer to your company guidelines on the format for each of these entries.

a. In the Organization field, enter your company name.

b. In the Unit field, enter descriptive information about the server.

Example: *business-unit*, *department*

c. Enter the location of the server.

Example: *building-name*, *floor*, *rack*

d. Enter the state in which the server is located.

You can enter an abbreviation or the full name for the state.

e. Select the country in which the server is located.

Enter the first letter of the country name, and use the up and down arrows to select the country. Then press the **Tab** key.

f. Select **OK**.

Step 11 In the Network Time Protocol Client Configuration screen, complete these steps:

a. Enter the same NTP server IP addresses, hostnames, or pool names that you configured for the database and call engine servers.

b. Take one of the following actions, the availability of which depends on whether you chose to enter the server information before or after installing the software in Step 3:

- Select **Test** to confirm connectivity to the NTP entries, and then select **Proceed**.
- Select **OK**.

Step 12 In the Security Configuration screen, enter the security password, confirm the password, and select **OK**.

Note You must configure the same security password on all database, administration, and call engine servers. After you configure the security password on a server, you cannot change it without reinstalling the server.

Caution This is your last chance in the installation wizard to select **Back** to verify your entries. Complete the next step only when you are sure that the entries that you made throughout this procedure are correct.

Step 13 In the Platform Configuration Confirmation screen, select **OK**.

If, in Step 3, you chose to proceed to enter the server information before installing the software, the following information applies:

- The installer spends approximately 30 minutes installing the software.
- If the system has problems with the information that you entered in the installation wizard, you will be prompted to correct the information.

The server ejects the installation DVD and reboots the server while completing the installation. This process takes approximately 10 minutes. When complete, the system prompts you to log in to the CLI.

```
The installation of Cisco TelePresence Exchange System has completed successfully.

Cisco TelePresence Exchange System x.x.x.x
hostname login:
```

What To Do Next

If you have not yet installed the software for the second administration server, do so now by repeating this procedure.

Otherwise, proceed to the "Checking the Administration Server Status and Network Connectivity" section on page 5-17.

Checking the Administration Server Status and Network Connectivity

Complete this task to confirm that the administration server is up and can connect to the other Cisco TelePresence Exchange System servers.

Procedure

Step 1 Log in to the CLI of the administration server.

```
Cisco TelePresence Exchange System x.x.x.x
hostname login: <username>
Password: <password>

Command Line Interface is starting up, please wait...

    Welcome to the Platform Command Line Interface

admin:
```

Step 2 To verify that the administration server is running, enter the **utils service adminserver status** command.

```
admin: utils service adminserver status
adminserver.................Running - PID <31650>
```

If the output does not indicate that the server is running, wait approximately 5 minutes for the server to finish coming up.

Step 3 To confirm that the administration server has network connectivity, enter the following command, specifying the IP or VIP address of any of the Cisco TelePresence Exchange System servers that are already installed:

utils network ping *ip-address*

The output confirms network connectivity:

```
admin: utils network ping 10.22.139.230
PING 10.22.139.230 (10.22.139.230) 56(84) bytes of data.
64 bytes from 10.22.139.230: icmp_seq=0 ttl=64 time=0.512 ms
64 bytes from 10.22.139.230: icmp_seq=1 ttl=64 time=0.093 ms
64 bytes from 10.22.139.230: icmp_seq=2 ttl=64 time=0.090 ms
64 bytes from 10.22.139.230: icmp_seq=3 ttl=64 time=0.090 ms
```

```
--- 10.22.139.230 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.090/0.196/0.512/0.182, pipe 2
```

Related Topics

- Appendix C, "Command Reference"

Verifying Data Connectivity Among the Servers

If the Cisco TelePresence Exchange System nodes are unable to properly exchange data, various problems will eventually arise. Complete this task to verify proper data connectivity after you install all six nodes in the Cisco TelePresence Exchange System server cluster or after you reinstall one of the nodes.

Procedure

Step 1 Point a web browser to the following URL, using the IP address of one of the administration servers:

http://*ip-address***/ctxadmin**

Make sure that you are not using the virtual IP (VIP) address that is configured on the Cisco Application Control Engine (ACE).

Step 2 If the login page for the Cisco TelePresence Exchange System administration console does not appear, complete the following steps:

a. Repeat Step 1, but this time use the IP address of the *other* administration server.

If the login page appears, proceed to Step 3.

b. Make sure that the browser machine can reach other devices in the same VLAN as the administration servers. Resolve any network connectivity issues.

c. Repeat Step 1.

Step 3 Log in to the administration console with the username **admin** and the password **cisco**.

Step 4 Select **System > Cluster Nodes**.

Step 5 Verify that all six nodes (two database servers, two call engine servers, and two administration servers) appear in the list of cluster nodes.

It may take up to five minutes for a newly installed node to register itself to the database and appear in the list of cluster nodes.

Step 6 If any of the servers remain missing from the list of cluster nodes, you need to reinstall those servers to correct the security password on those servers.

Complete the procedures that are relevant to the servers that are missing from the list of cluster nodes:

- Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers, page 5-4
- Installing the Cisco TelePresence Exchange System Call Engine Servers, page 5-9
- Installing the Cisco TelePresence Exchange System Administration Servers, page 5-14

CHAPTER 6

Upgrading the Software

The following topics describe how to upgrade the software on the Cisco TelePresence Exchange System:

Requirements for Upgrading the Software

- All six nodes in the server cluster must run the exact same software version.

  See the *Release Notes for the Cisco TelePresence Exchange System* for your specific release for any restrictions on software version compatibility. The release notes are available at http://www.cisco.com/go/ctx-relnotes.

- You must download the applicable tar.gz files from Cisco.com before you start the upgrade process. Then, copy these tar.gz files to your own designated SSH File Transfer Protocol (SFTP) server.

  See the *Release Notes for the Cisco TelePresence Exchange System* for your specific release for the actual release version to download.

Task List for Upgrading the Software

You must perform the upgrade process in the following order:

1. Contact the Cisco TAC and TME teams to install the upgrade user interface (UI) patch file by connecting to each node by using a remote account through Secure Shell (SSH). This patch installation procedure is independent of the actual upgrade window and can be done any time.

Note This procedure is applicable only to Cisco TelePresence Exchange System release 1.0.(x). To upgrade to subsequent releases, this procedure installs an upgrade UI patch to release 1.0.(x). However, this procedure is not required for initial installations of release 1.1.(x) or later.

2. Perform a database backup using the user interface of the Cisco TelePresence Exchange System Administrative Console. For detailed information about how to perform a database backup, see the "Configuring System Settings" chapter.

3. Perform the actual upgrade for all six nodes from the upgrade user interface (see "Upgrading the Database, Administration, and Call Engine Servers" section on page 6-3).

Managing the Software Upgrade

The following topics describe how to manage the software upgrade process:

Accessing the Upgrade Window

Procedure

To access the Cisco TelePresence Exchange System window, do the following procedure:

Step 1 If you are upgrading from a previous release, browse to https://<*IP address of the administration server*>:9010/ctx-upgrade-admin.

The login window of the Cisco TelePresence Exchange System Upgrade displays.

Step 2 Enter the Administrator Login username and password that you use for command line interface (CLI) access. (The Administrator Login username and password are specified during installation.) Then, click **Log In**.

Note Be aware that these user credentials are different from the credentials used to access the administration console.

Step 3 Follow the online security instructions for your supported browser.

The Cisco TelePresence Exchange System Upgrade window displays.

The **Upgrade** link displays in the banner pane each time you access the administration console, and only if you want to upgrade.

Navigation Pane of the Upgrade Window

The navigation pane is on the left side of the upgrade window. The navigation pane lists the tasks that you need to perform during the upgrade process. After each task is completed successfully, the system automatically takes you to the next task. Table 6-1 describes the tasks of the navigation pane of the upgrade window.

Table 6-1 Upgrade Tasks

Task	Description
Node Sequence	Selecting three nodes to upgrade first. You must select one database node, one administration node, and one call engine node.
Patch File	Transferring the upgrade bundle patch file to all six nodes.
Validation	Validating that each node in the cluster is ready and that the MD5 checksum is correct.
Side A Maintenance	Placing the three nodes for Side A in maintenance mode.
Side A Installation	Installing the patch file for each of the three nodes for Side A.
Side B Maintenance	Placing the remaining three nodes for Side B in to maintenance mode.
Database Migration	Migrating the contents from the Side B database from the previous version over to the Side A database.
Side A Online	Bringing each of the three nodes for Side A out of maintenance mode to standalone mode with the upgraded version.
Side B Installation	Installing the patch file for each of the three nodes for Side B.
Side B Online	Bringing each of the three nodes for Side B online.

Upgrading the Database, Administration, and Call Engine Servers

Before You Begin

- If possible, block users from scheduling meetings that will occur during this upgrade period.
- If possible, you should notify all users about your system downtime before you start the upgrade process.
- Verify that both database servers are synchronized.
- Verify that you have copied the upgrade bundle patch file to your own designated SFTP server.
- At a minimum, allow at least three hours to complete the actual upgrade on all of the administration, database, and call engine servers. However, the actual system downtime is less than 30 minutes.
- Verify the state of each node by accessing the CLI. For information about the commands, see the "Command Reference" appendix.

  For a production system, you must test system usability.
- Verify that the database is backed up to an external server.
- We recommend that you schedule a meeting to make sure that the previous release version is working properly.
- Specify the meeting names when you are upgrading from the previous release to the current release. You should also verify that the existing meeting names are overwritten during the upgrade.
- Verify that all six nodes are displayed as online in the Cisco TelePresence Exchange System Upgrade window. If a node is displayed as offline, bring the node back online and verify connectivity.
- Verify that you have retrieved all call detail records and associated event records. Any previous records that remain will be purged during the upgrade process.

- Verify that the IP address can be directly reached for the two administration servers. During the upgrade process, you are required to access a specific administration server.
- By default, only CTS endpoints may join meetings hosted on a Cisco TelePresence Multipoint Switch. For new installations, the *Installation and Administration Guide for the Cisco TelePresence Exchange System Release 1.1* includes instructions on enabling these types of endpoints when you configure the Cisco TelePresence Multipoint Switch to work with the Cisco TelePresence Exchange System.

  If you have already configured a Cisco TelePresence Multipoint Switch to work with the Cisco TelePresence Exchange System, see the "Enabling Cisco TelePresence Endpoints Running TC Release 5.x to Join Meetings Hosted on the Cisco TelePresence Multipoint Switch" section on page 16-18.

Procedure

Note
- During the entire upgrade process, all provisioning data is saved.
- If you cancel the operation from Step 2 to Step 5, all of your changes will be reverted before you return back to the Cisco TelePresence Exchange System Upgrade window. If you cancel the operation from Step 7 to Step 10, the system reverts back to the original state on Side B. The system is placed in nonredundant mode because only one side is active. Once both sides are upgraded, you cannot revert back from the user interface.

To upgrade the database, administration, and call engine servers, do the following procedure:

Step 1 To begin the upgrade process, click **Start**.

In the navigation pane, the **Node Sequence** option is highlighted.

Step 2 To start the tasks for the Node Sequence option, do the following steps:

a. In the Node Sequence option, select one of each type of node to upgrade first.

This selection is the primary role and named Side A. The remaining three nodes are upgraded second and named Side B.

Note Side A cannot be assigned a database node with a primary role.

b. To save the node sequence selections, click **Save Node Sequence**.

To cancel the operation and return back to the Cisco TelePresence Exchange System Upgrade window, click **Cancel**.

Note You are not allowed to cancel an operation while it is in progress.

In the navigation pane, the **Patch File** option is highlighted.

Step 3 To transfer the upgrade bundle patch file from your own designated SFTP server, do the following steps:

a. In the URL field, enter the applicable IP address of the SFTP server and the location of the upgrade bundle patch file.

Note You are using the same upgrade bundle patch file that you previously downloaded.

b. In the Credentials field, enter your SFTP username and password.

c. To start the transfer process, click **Begin Transferring**.

The upgrade bundle patch file is downloaded from the specified SFTP server. Then, this file is uploaded automatically to all six nodes. When complete, a green check mark is displayed for each of the six nodes.

To cancel the operation and return back to the Cisco TelePresence Exchange System Upgrade window, click **Cancel**.

Note You are not allowed to cancel an operation while it is in progress.

In the navigation pane, the **Validation** option is highlighted.

Step 4 To validate that each node in the cluster is ready to get upgraded, migrated, and that the MD5 checksum of the patch file matches with the MD5 checksum that you downloaded, do the following steps:

a. To start the validation process for the cluster, click **Validate Cluster**.

When complete, a green check mark is displayed for each of the six nodes and the patch file for the MD5 check sum.

If you receive an error that a node cannot be migrated, notify Cisco TAC immediately.

A health check on one or more nodes could fail if a process was not running or if the database servers are not synchronized. If the process was stopped manually, you need to start it. If the database servers display an error, complete the split brain recovery procedure. For more information about this procedure, see the "Split Brain Recovery" chapter.

b. To confirm that you have manually validated that the displayed MD5 checksum matches the MD5 checksum displayed from the Cisco.com download site, click **Checksum Is Correct**.

The system obtains the MD5 checksum from each of the six nodes, and validates that the MD5 checksum is the same on each node. Then, the MD5 checksum is displayed in the Validation window.

If the MD5 checksums do not match, do not proceed and restart the upgrade.

To cancel the operation and return back to the Cisco TelePresence Exchange System Upgrade window, click **Cancel**.

Note You are not allowed to cancel an operation while it is in progress.

In the navigation pane, the **Side A Maintenance** option is highlighted.

Step 5 To place the three nodes for Side A in maintenance mode, click **Put Side A Nodes Into Maintenance Mode**.

The other three nodes for Side B continue to handle calls in standalone mode. When complete, a green check mark is displayed for each of the three nodes for Side A.

To cancel the operation and return back to the Cisco TelePresence Exchange System Upgrade window, click **Cancel**.

Note We recommend that you do not cancel this operation.

In the navigation pane, the **Side A Installation option** is highlighted.

Step 6 To install the patch file for each of the three nodes for Side A, click **Install Patch On Side A**.

After the installation, these nodes are rebooted and the new version is in maintenance mode. When complete, a green check mark is displayed for each of the three nodes for Side A.

This process involves installing new software on all of the Side A nodes and rebooting them. If an older firmware version is detected during a reboot, it is also upgraded. During the firmware update process, the machine reboots four times.

Note This process takes approximately one hour. If a firmware upgrade is also required, this process takes approximately two hours.

If you want to cancel the operation, revert the system back to nonredundant mode, and return back to the Cisco TelePresence Exchange System Upgrade window, click **Cancel**.

Note We recommend that you do not cancel this operation.

In the navigation pane, the **Side B Maintenance** option is highlighted.

Step 7 To place the remaining three nodes for Side B in to maintenance mode, click **Put Side B Nodes Into Maintenance Mode**.

Note During this process, the entire system is offline. All new calls will fail and existing calls will drop.

To cancel the operation and return back to the Cisco TelePresence Exchange System Upgrade window, click **Cancel**.

Note We recommend that you do not cancel this operation.

In the navigation pane, the **Database Migration** option is highlighted.

Step 8 To migrate the contents from the Side B database from the previous version over to the Side A database, click **Migrate Database**.

Note Depending on how much data that you need to migrate, this process may take more than five minutes.

To cancel the operation and return back to the Cisco TelePresence Exchange System Upgrade window, click **Cancel**.

Note We recommend that you do not cancel this operation.

In the navigation pane, the **Side A Online** option is highlighted.

Step 9 To bring each of the three nodes for Side A out of maintenance mode to standalone mode with the upgraded version, click **Bring Side A Online**.

When the Side A nodes are online, these nodes can handle calls. The system operates in a nonredundant state.

If you want to cancel the operation, click **Cancel**.

In the navigation pane, the **Side B Installation** option is highlighted.

Note Before you start the process to install Side B, make sure that Side A is handling calls and scheduling meetings properly.

Step 10 To install the patch file for each of the three nodes for Side B, do the following steps:

a. To start the patch installation process for these three nodes, click **Install Patch On Side B**.

After the installation, the nodes for Side B are rebooted and the new version is in maintenance mode.

This process involves installing new software on all of the Side B nodes and rebooting them. If an older firmware version is detected during a reboot, it is also upgraded. During the firmware update process, the machine reboots four times.

Note This process takes approximately one hour. If a firmware upgrade is also required, this process takes approximately two hours.

The system displays a message prompting you to confirm that you want to log in to Side A while Side B is being upgraded and restarted.

b. To confirm, click **Continue to Side A**.

When complete, a green check mark is displayed for each of the three nodes for Side B.

Note If the operation is cancelled, notify Cisco TAC immediately.

In the navigation pane, the **Side B Online** option is highlighted.

Step 11 To bring each of the three nodes for Side B online, click **Bring Side B Online**.

When the Side B nodes are online, the system operates in a redundant state.

A success message displays informing you that the cluster nodes are online. The running version also displays. You can verify the status of each node by accessing the CLI. For information about the commands, see the "Command Reference" appendix.

Step 12 To return to the Cisco TelePresence Exchange System Upgrade window, click **Return to Overview**.

Related Topics

- Appendix C, "Command Reference"

PART 3

Configuring the Cisco TelePresence Exchange System

CHAPTER 7

Getting Started with Configuration

This section provides information about the basic configuration tasks for setting up the different types of meeting service offered by the Cisco TelePresence Exchange System.

This section includes the following topics:

Prerequisites for Configuring the Cisco TelePresence Exchange System

Before configuring the Cisco TelePresence Exchange System, ensure that you install and configure the following:

- Cisco router to function as a SBC
- Cisco Application Control Engine (ACE)
- Cisco TelePresence Multipoint Switch
- Cisco TelePresence MSE 8000 Series system
- Cisco router with integrated video response (IVR) capabilities
- Cisco Unified Communications Manager
- Cisco TelePresence Manager—Required for OBTP only.
- Cisco Catalyst Switch that provides Layer 2/ 3 connectivity for the Cisco TelePresence Exchange System and the other Cisco platforms.

For instructions on how to configure the external network components with which the Cisco TelePresence Exchange System interacts, see the corresponding chapters in the "Configuring External Network Components for Cisco TelePresence Exchange System" part of this guide.

Configuration Task Lists for Setting Up Meeting Services

The configuration task lists provided in this section describe how to set up the basic features for different types of meeting services offered by the Cisco TelePresence Exchange System. As dependencies exist between some configuration tasks, we recommend that you perform the configuration tasks for each type of meeting service in the order presented in the following sections.

Prerequisites for Setting Up Meeting Services

Before setting up the Cisco TelePresence Exchange System meeting services, do the initial configuration tasks in the following order:

1. Modify default user settings.
2. Create the service provider.
3. Verify that the required product licenses are active.

Setting Up the Meet-Me and Rendezvous Meeting Service

A Meet-Me meeting is hosted by this Cisco TelePresence Exchange System to provide a scheduled meeting for two or more Cisco TelePresence or third-party endpoints. Unlike a Meet-Me meeting, a Rendezvous meeting (also called a *timeless* or *reservationless* meeting) is not limited to a single start time. To set up the Meet-Me and Rendezvous meeting service, do the associated configuration tasks in the following sections:

Note The same configuration steps may apply to more than one type of meeting service.

1. "Configuring Media Resources" section on page 7-3—Required for both dial in and dial out calls.
2. "Configuring Customers" section on page 7-4—Required for dial out calls only.
3. "Configuring Call Routing" section on page 7-4—Required for both dial in and dial out calls.

Setting Up the Remote Service Provider Meeting Service

A remote service provider meeting is hosted by a remote Cisco TelePresence Exchange System. The Cisco TelePresence Exchange System does not reserve any media resources for a remote service provider meeting. To set up the remote service provider meeting service, do the associated configuration tasks in the following section:

Note The same configuration steps may apply to more than one type of meeting service.

- "Configuring Call Routing" section on page 7-4

Setting Up the Direct Dial Meeting Service

A direct dial meeting is a scheduled meeting between two hosted provisioned endpoints. The Cisco TelePresence Exchange System does not reserve any media resources for a direct dial meeting. To set up the direct dial meeting service, do the associated configuration tasks in the following sections:

Note The same configuration steps may apply to more than one type of meeting service.

1. "Configuring Customers" section on page 7-4
2. "Configuring Call Routing" section on page 7-4
3. "Configuring Whitelisting" section on page 7-5

Performing Additional Configuration Tasks

After setting up the basic features for the different types of meeting service offered by the Cisco TelePresence Exchange System, you can perform, for example, the following configuration tasks to enhance the functionality of Meet-Me and Rendezvous meeting service:

- Customize IVR prompts.
- Configure SIP route for help desk calls.
- Configure provisioned endpoints for OBTP.

Configuration Tasks for Setting Up Meeting Services

Before performing the configuration tasks described in the following sections, see the "Configuration Task Lists for Setting Up Meeting Services" section on page 7-2 for guidance:

- Configuring Media Resources, page 7-3
- Configuring Customers, page 7-4
- Configuring Call Routing, page 7-4
- Configuring Whitelisting, page 7-5

Configuring Media Resources

To configure the media resources for Meet-Me and Rendezvous meeting service, do the configuration tasks in the following order:

1. Define a region.

   For more information, see the "Configuring Regions" section.

2. Configure reservations types.

   For more information, see the "Configuring Reservation Types" section.

3. Configure resource groups.

   For more information, see the "Configuring Resource Groups" section.

4. Configure IVR resources for the region.

   For more information, see the "Configuring IVR Resources" section.

5. Configure the CTMS resource.

   For more information, see the "Configuring CTMS Resources" section.

6. Configure the Cisco TelePresence MCU MSE 8510 resource.

   For more information, see the "Configuring MSE 8510 Resources" section.

7. Configure the Cisco TelePresence Server MSE 8710 resource.

   For more information, see the "Configuring TPS Resources" section.

Configuring Customers

To configure customers for direct dial meeting service and Meet-Me and Rendezvous dial out meeting service, do the configuration tasks in the following order:

1. Configure the organizations.

   For more information, see the "Configuring Organizations" section.

2. Configure the endpoints.

   For more information, see the "Configuring Endpoints" section.

Configuring Call Routing

Dial In Routing

To configure call routing for Meet-me and Rendezvous dial in meeting service, do the following configuration task:

1. Configure a service number for the service provider.

   For more information, see the "Configuring Service Numbers" section.

SIP Dial Out, Remote Service Provider, and Direct Dial Routing

To configure call routing for Meet-me and Rendezvous dial out, remote service provider, and direct dial meeting services, do the configuration tasks in the following order:

1. Configure the SIP resource.

   For more information, see the "Configuring SIP Resources" section.

2. Configure an organization or remote service provider.

   For more information, see the "Configuring Organizations" section or the "Configuring Remote Service Providers" section.

3. Configure a SIP route for each organization or remote service provider.

   For more information, see the "Configuring Routes" section.

4. (Optional) Configure a dial pattern for each organization or remote service provider.

   For more information, see the "Configuring Dial Patterns" section.

5. Edit defined organization or remote service provider to associate them with defined SIP route and dial pattern.

   For more information, see the "Configuring Organizations" section or the "Configuring Remote Service Providers" section.

Configuring Whitelisting

Note You must configure call routing for direct dial meeting service before configuring whitelisting.

To configure whitelisting for direct dial meeting service, do the configuration tasks in the following order:

1. Configure whitelist settings for each organization.

   For more information, see the "Configuring Organizations" section.

2. Configure whitelist groups.

   For more information, see the "Configuring Whitelist Groups" section.

CHAPTER 8

Configuring System Settings

The administration console shows the status of key system functions. The following sections describe the system status display and how to configure system settings:

Understanding System Status

The administration console home page displays the system configuration status for the following key functions:

- Scheduling—Configuration required before you can schedule meetings.
- Attending—Configuration required before anyone can attend meetings.
- OBTP—Configuration required for One-Button-to-Push (OBTP) functionality.
- System—Cisco TelePresence Exchange System will only launch meetings if valid licenses are provisioned.

A green check-mark icon next to the function indicates that the system configuration is complete for the corresponding function. A red stop-sign icon indicates that the system configuration is missing or incomplete for the corresponding function.

If any of the key functions display a red icon, the What's Wrong field provides a description of the configuration issue that needs to be addressed. Click the fix link (the button with the hammer icon) to open the configuration page on which the issue can be resolved.

Note The system configuration status also is displayed in the System Status panel (below the navigation pane) on all administration console pages.

Note The system status display refreshes each time that you navigate to a new page.

Resource Operational States

The live system ping displays the overall health of the other platforms that communicate with the Cisco TelePresence Exchange System. The system monitors these platforms by sending status messages periodically. Systems that respond to the message display a green icon and systems that are not responding to the message display a red icon. Systems that are in maintenance mode display a yellow icon.

Understanding Alarms

You can use the Alarms window to get a detailed view of system health, and as a starting point when debugging system errors or failures.

The Cisco TelePresence Exchange System retains alarm details for up to 30 days from the time the alarm was generated. The system automatically purges alarms that exceed this 30-day limit. If the total number of alarms retained by the system reaches 100,000, the system retains only the most recent 100,000 alarms and automatically purges the rest.

Procedure

To view and filter alarms for the system, do the following procedure:

Step 1 From the navigation pane, choose **System > Alarms**.

The Alarms window is displayed showing details on alarms for the past 30 days.

Fields on the **System > Alarms** window are described in Table 8-1.

Step 2 To view more information about a specific alarm, click anywhere in the alarm row.

Alarm details are listed on the right side of the window.

Step 3 (Optional) To filter the information that is displayed on the Alarms window, do one of the following:

- To filter on the Severity information that is displayed on the Alarms window, click the T icon next to the column heading, and check the check boxes next to each item that you want to display on the window.

  To display Alarms for all items, check All.
- To filter on any specific heading other than Severity, click the T icon next to the column heading, and enter the specific item on which you want to filter.

Step 4 To activate the filter, click **Filter**.

To deactivate a filter, click the **T** icon next to the appropriate column heading and click Clear.

Note When you click **Clear Filters**, the system clears all defined filters.

Table 8-1 Alarms Field Descriptions

Field	Description
Severity	Text description and icon indicating the level of severity of the alarm. (Levels range from Emergency to Info.)
Time	Time and date stamp indicating when the alarm was generated.
Summary	Text description of the alarm.
Server	Name of the server on which the alarm occurred.

Understanding Cluster Nodes

The Cisco TelePresence Exchange System is a cluster node, which is composed of at least two administration servers, two call engines, and two database engines.

After installation of a Cisco TelePresence Exchange System completes, the cluster node registers itself to the database (every five minutes). When the administration server discovers the new cluster node, it appears in the cluster node list within the administration console.

Fields on the **System > Cluster Nodes** window are described in Table 8-2.

Table 8-2 Cluster Node Field Descriptions

Field	Description
Node Name	Node name of the node. Click the node name to view only the information for that node.
Host Name	Hostname of the node.
IP Address	The IP address of the node. See the "Common Field Properties" section on page 2-4.
Cluster	Name of the cluster to which the node belongs. Currently, **Default Cluster** is the only cluster name.
Operational State	The current operational state of the node: Offline, Online, Maintenance or Unknown.
Node Type	The server type of the node: ADMIN, ENGINE, or DATABASE.

Configuring Time Zones

You can activate any number of time zones for the administration console. All of the supported time zones are listed alphabetically on the System > Time Zones page by continent and city. A time zone with a check in the Active check box is active and assignable by the system within various configuration panels of the administration console.

You must activate a time zone to allow configuration of the time of day within the administration console such as setting the starting time for a meeting. You also choose a time zone from the list of activated time zones when scheduling backups.

When creating or editing a user, you can assign the user any activated time zone. The user sees alarms, diagnostics, and other time displays in the selected time zone when using the administration console, and the time zone is selected by default when the user schedules meetings.

Procedure

To activate a time zone, do the following procedure:

Step 1 From the navigation pane, choose **System > Time Zones**.

The Time Zones window is displayed.

Step 2 To activate a time zone, check the **Active** check box next to the desired time zone.

The time zone is now active.

Step 3 To determine which time zones are active, click the **T** icon next to the Active heading.

Step 4 In the panel that is displayed, check the **Active** check box and click **Filter**.

Configuring Users

Topics in this section include:

Adding Users

Before You Begin

Configure the time zones served by this Cisco TelePresence Exchange System.

Only system administrators can modify user settings.

Procedure

To add a new user, do the following procedure:

Step 1 From the navigation pane, choose **System > Users**.

The Users window is displayed.

Step 2 Click **Add A New User**.

Step 3 Enter the settings as indicated in Table 8-3 to configure the user.

Step 4 To save your changes, click **Save**.

Editing User Settings

Before You Begin

Only system administrators can modify user settings.

Procedure

To edit user settings, do the following procedure:

Step 1 From the navigation pane, choose **System > Users**.

The Users window is displayed.

Step 2 In the item table, click the applicable user ID.

The User Details window is displayed.

Tip You can also reach the User Details window for the account that you used to log in by clicking the username link in the banner pane. For more details, see the "Banner Pane" section on page 2-2.

Step 3 From the toolbar, click **Edit This User**.

The Edit User window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as required.

Fields are described in Table 8-3.

Step 5 To save your changes, click **Save**.

Deleting Users

Before You Begin

Only system administrators can delete users.

Procedure

To delete a user, do the following procedure:

Step 1 From the navigation pane, choose **System > Users**.

The Users window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple users at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a user prior to deleting it, in the Users window, you can click the applicable **User ID** to go to the User page. After verifying that you have chosen the correct user to delete, click **Delete This User**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

User Fields

Table 8-3 User Field Descriptions

Field	Description
First Name	The first name of the user. See the "Common Field Properties" section on page 2-4.
Last Name	The last name of the user. See the "Common Field Properties" section on page 2-4.
User ID	Unique ID assigned to this user. The user enters the user ID when logging in to the administration console.
Email Address	Email address of the user.
Password	Password assigned to the user during system installation or by the system administrator. The user enters the password when logging in to the administration console.
Verify Password	Password entered again for verification.
Role	See the "User Roles" section on page 8-6.
Timezone	Drop-down list displays the active time zones. Choose the time zone that matches the location of the user. See the "Configuring Time Zones" section on page 8-3.

User Roles

Table 8-4 lists the roles that you can assign to users in the Cisco TelePresence Exchange System administration console.

Table 8-4 User Roles

Role	Privileges
SYSTEM system administrator	System administrators can configure all system settings in the admin console and can add new users of any role.
ADMIN administrator	Administrators can configure all system settings in the admin console and can add only new API users.

Table 8-4 User Roles (continued)

Role	Privileges
PROVISIONING provisioning user	Provisioning users can configure only the settings in the Customers and Endpoint Management areas of the admin console. For all other pages in the admin console, provisioning users have read-only privileges.
READONLY read-only user	Read-only users can view but not edit any pages of the admin console.
API API user	Unlike the other user roles, the API role is assigned to billing and operational systems instead of people. The API user role allows other systems to access the Cisco TelePresence Exchange System API. The API user role does not allow access to the admin console.
SERVICEDESK service desk user	Service desk users can schedule, modify, and cancel meetings. Users with this role can also manage Meet-Me and Rendezvous meetings that are currently in progress, performing functions such as muting or unmuting participants, dialing out to additional endpoints, or increasing the duration of the meeting. Users with this role have view-only access to other areas of the administration console.

Related Topics

- *API User Guide for the Cisco TelePresence Exchange System*, available at http://www.cisco.com/en/US/products/ps11276/products_programming_reference_guides_list.html.
- Managing Active Meetings, page 13-32

Configuring Database Backups

You can configure regular backups of the database server that run automatically at scheduled times, or you can do a manual, on-demand backup as needed.

After each database backup completes, the system marks the backup attempt with one of the following statuses in the Status column of the Database Backup window: success, failed, missing (server cannot find file to delete), or deleted.

When a database backup is in process, the system notes the status as In Progress.

When the system (or administrator) cancels a database backup, the system notes the status as Cancelled.

Retention Policy

You can define how many copies of database backups that you retain, and define the retention method in terms of backup number, size (MB), and time (days). You can define multiple retention methods.

When the number of database backups exceeds the retention policy settings, the system deletes database backups in accordance with the following rules:

- The system applies the retention policy during each database backup.
- The system deletes the oldest successful backup first.

- When there are multiple retention policies in use, the system deletes the oldest successful backup that exists among all defined policies.
- No system warning is given before the database backup deletion occurs.

Note

- Cisco recommends that the administrator not perform manual deletions of database backup files on the server. Manual deletions can cause the defined retention policy to delete more database backup files than necessary.
- For details on reviewing the number of database backups stored on the backup server, see the "Viewing Past Database Server Backups and Restores" section on page 24-1.
- For details on running a manual backup or restoring a backup to a database server, see the "Managing Database Backups" chapter.

Before You Begin

Create a directory on a server on which you can save the database backups.

Ensure that you have the log in information (username and password) for the server on which you are saving the database backups.

Test access to the designated backup server by using either FTP or SFTP.

Procedure

To configure a database backup, do the following procedure:

Step 1 From the navigation pane, choose **System > Database Backup**.

The Backup Summary window is displayed.

Step 2 To configure a backup, click **Configure Backups** (near the top of the window).

Step 3 To indicate how often you want the backup to automatically run, select one of the following options:

- To do a database backup at the same time each day, click the **Daily at** radio button.
- To do a database backup at the same time for multiple days during the week, click the **Weekly on** radio button, and then check the check box next to the days of the week that you want the automatic backup to run.

Step 4 In the two **at** fields, enter the time of day that you want the backup to run (such as 2:00).

Step 5 From the drop-down list next to the time of day entry fields, choose either **AM** or **PM**.

Step 6 From the drop-down list next to the AM/PM drop-down list, choose the time zone.

Step 7 To enter details for the server on which you want to save the database backup, enter the following:

a. Enter either the server name (if DNS is in use) or the IP address.

b. Enter the directory path to the server.

c. Enter the username and password for the server.

d. Choose the transfer protocol from the drop-down list.

e. Enter the port number.

By default, the port number field auto-populates with one of the following port numbers to match the transfer protocol that you select in Step 7d.

When you select FTP as the transfer protocol, the port number 21 auto-populates.

When you select SFTP as the transfer protocol, the port number 22 auto-populates.

Step 8 To define a retention policy for the database backups, choose one or more of the following options:

- To define the number of database backups that you want to save, check the **This many backups** check box and enter a number in the field.
- To place a size limit on the memory that is allocated for the database backups on the server, check the **Until total size reaches** check box, and then enter the appropriate number in the MB field.

Note Although the size of a database file can increase as a system gathers more logs, Cisco recommends that the administrator plan for a database file of approximately 400 MB per backup.

- To save database backups for a set number of days, check the **Backups for up to** check box, and then enter a number in the days field.

Step 9 To save your configuration, click **Save**.

Note If you modified the field for the path, a warning message is displayed to inform you that the system is attempting to move the files from the previous path to the new one. If you modified the field for the host, the system does not attempt to move the files.

Step 10 (Optional) Click **Synchronize Server Status**.

If the system cannot locate the backup file on the new server, the system does not mark the file as missing at that time. Instead, the system preserves the historical backup entries that are associated with that backup. The system remembers that the backup was successful on that particular server.

If the system locates the backup file from the previous host on the new server, the backup entry is updated to display the presence on the new server.

Understanding Backward Compatibility

Release 1.1 is backward compatible with Release 1.0. This means that you can use the Release 1.0 APIs with a Release 1.1 system.

For information on using backward compatibility, refer to the *API User Guide for the Cisco TelePresence Exchange System*, available at http://www.cisco.com/en/US/products/ps11276/products_programming_reference_guides_list.html.

Changing Global Configuration Settings

Global Configuration settings are those which apply to the system as a whole, rather than to a specific entity such as a service provider, organization, or meeting.

The following sections describe how to configure these global configuration settings:

- Configuring Number of Rows to Display Per List Page, page 8-10
- Configuring Meet-Me Default Screens, page 8-10

Configuring Number of Rows to Display Per List Page

You can control the number of rows that display on the page at one time in lists in the administration console (for example, on the Alarms, Time Zones, or Meetings list pages) by changing the value of the Number of Rows to Display Per List Page field. The new value takes effect for all users of the administration console.

Procedure

To configure the Number of Rows to Display Per List Page setting, do the following procedure:

Step 1 From the navigation pane, choose **System > Global Configuration**.

The Global Configuration window is displayed.

Step 2 Modify the Number of Rows to Display Per List Page field value as required.

Fields on the page are described in Table 8-5.

Step 3 To save your changes, click **Save**.

The change takes effect immediately after you save the page.

Configuring Meet-Me Default Screens

The MeetMe Default Screens global setting allows you control over the number of segments that the system reserves for unprovisioned endpoints that do not have a media profile associated with them (in other words, for dial-in calls or for dial-out situations where no media profile is specified by the meeting scheduler). In these cases, if the meeting is hosted on a CTMS bridge, the system reserves MeetMe Default Screens + 1 segments (the additional segment is to account for the possibility of 30 FPS presentation sharing). If the meeting is hosted on a TPS bridge, the system reserves MeetMe Default Screens. The system always reserves one screen for these endpoints on an MCU MSE 8510 bridge.

The value of MeetMe Default Screens is also used to calculate the amount of capacity to reserve for a Rendezvous meeting. In this case, the system multiplies the value that you specify for Number of Endpoints by a fixed number of segments for the type of bridge (MeetMe Default Screens + 1 for CTMS, MeetMe Default Screens for TPS, and 1 for MSE 8510). This gives a “worst-case” estimation assuming that all endpoints that join will use the same amount of bandwidth. The system then adds the value of the Additional Capacity field on to the total.

Note Lowering the MeetMe Default Screens value may cause capacity problems for all meetings concurrently hosted on the bridge if unprovisioned endpoints with more screens than are reserved join the meeting. We recommend that you provision all endpoints that have more screens than the MeetMe Default Screens value.

At attend time, the system uses the value of MeetMe Default Screens to determine the number of segments to allocate when an unprovisioned or remote endpoint joins the meeting, using the same bridge type-based calculation (MeetMe Default Screens + 1 for CTMS, MeetMe Default Screens for TPS, or 1 for MSE 8510).

For more information on capacity reservation and allocation, see Appendix B, "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection."

Procedure

To configure MeetMe Default Screens, do the following procedure:

Step 1 From the navigation pane, choose **System > Global Configuration**.

The Global Configuration window is displayed.

Step 2 Modify the MeetMe Default Screens field value as required.

Fields on the page are described in Table 8-5.

Step 3 To save your changes, click **Save**.

Step 4 After saving your changes, restart the call engine servers in order for the change to take effect.

Configuring the SIP Load Balancer Address

The administrator defines the SIP load-balancer address for call engines that employ the ACE for redundancy. Generally, the administrator defines the SIP load-balancer address on the system after installation and in situations in which the IP address of the call engines or the ACE changes.

Procedure

To configure a SIP Load Balancer Address, do the following procedure:

Step 1 From the navigation pane, choose **System > Global Configuration**.

The Global Configuration window is displayed.

Step 2 Modify the SIP Load Balancer Address field value as required.

Fields on the page are described in Table 8-5.

Step 3 To save your changes, click **Save**.

Step 4 After saving your changes, restart the call engine servers in order for the change to take effect.

Configuring an ISDN Dial Out Prefix

When you define an ISDN Dialout Prefix value, the system adds a prefix to the beginning of all ISDN dial out calls. For example, if the endpoint number is 4013164407 and the defined ISDN prefix number is 9, then the call will be sent out as 94013164407.

The Cisco VCS call manager references the ISDN Dialout Prefix to determine whether to send the call to the ISDN gateway. If the configured ISDN Dialout Prefix does not match the value that is configured within the Cisco VCS, then all ISDN dial outs fail. When the call is sent to the ISDN gateway, the ISDN prefix is removed, restoring the original number.

The system default for the ISDN Dialout Prefix is 9. The administrator can modify the default ISDN Dialout Prefix setting when the value of 9 is already in use by another system, or to match a different value that is set in the Cisco VCS.

Note The ISDN Dialout Prefix must not match the prefix of any provisioned or unprovisioned endpoints. If the prefixes match, the Cisco TelePresence Exchange System will not properly recognize the endpoint, causing problems such as failure to start a meeting if the endpoint is configured as a host.

Note ISDN calls may fail if the ISDN Dialout Prefix is set to null or does not match the value that is configured within the Cisco VCS.

Procedure

To configure an ISDN dial out prefix other than the system default value of 9, do the following procedure:

Step 1 From the navigation pane, choose **System > Global Configuration**.

The Global Configuration window is displayed.

Step 2 Modify the ISDN Dialout Prefix field value as required.

Fields on the page are described in Table 8-5.

Step 3 To save your changes, click **Save**.

Step 4 After saving your changes, restart the call engine servers in order for the change to take effect.

Global Configuration Fields

Table 8-5 Global Configuration Field Descriptions

Field	Description
Number of Rows to Display Per List Page	The number of rows that display on the page at one time in lists in the administration console (for example, on the Alarms, Time Zones, or Meetings list pages). The range of this field is 10 to 100. The default value is 20 items.
MeetMe Default Screens	Enter a value which the Cisco TelePresence Exchange System uses to calculate the number of segments to reserve for unprovisioned endpoints that do not have a media profile associated with them (in other words, for dial-in calls or for dial-out situations where no media profile is specified by the meeting scheduler). The system calculates the number of segments based on the type of media bridge resource that is scheduled to host the meeting, as follows: • CTMS—MeetMe Default Screens +1 • TPS—MeetMe Default Screens • MCU MSE 8510—1 segment, regardless of this value. For Rendezvous meetings, the system multiplies the value that you specify for Number of Endpoints by the same bridge type-based calculation as above (MeetMe Default Screens + 1 for CTMS, MeetMe Default Screens for TPS, and 1 for MSE 8510) and then adds the value of the Additional Capacity field to calculate the total capacity to reserve. **Note** Lowering the MeetMe Default Screens value may cause capacity problems on the bridge if unprovisioned endpoints with more screens than are reserved join the meeting. At attend time, the system uses the value of MeetMe Default Screens to determine the number of segments to allocate when an unprovisioned or remote endpoint joins the meeting, using the same bridge type-based calculation (MeetMe Default Screens + 1 for CTMS, MeetMe Default Screens for TPS, or 1 for MSE 8510).
SIP Load Balancer Address	Enter the address used to load balance SIP messages for call engines that employ the Cisco Application Control Engine (ACE) for redundancy. You typically enter the SIP load-balancer address on the system after installation and in situations in which the IP address of the call engines or the ACE changes.
ISDN Dialout Prefix	By default, the ISDN Dialout Prefix value is 9. The value must match the setting in the Cisco TelePresence Video Communication Server (Cisco VCS), and must not match the prefix of any provisioned or unprovisioned endpoints.

CHAPTER 9

Configuring Media Resources

The Cisco TelePresence Exchange System uses media resources on several Cisco platforms. The following sections describe how to configure the media resources:

Configuring IVR Resources

To provide IVR prompts to the user, the Cisco TelePresence Exchange System uses IVR resources on a Cisco router in the network. You need to configure information about the Cisco router used by this Cisco TelePresence Exchange System.

The following sections describe how to configure IVR resources:

Adding IVR Resources

Before You Begin

Install and configure the Cisco router with IVR capabilities. For additional information, see the "Configuring the Cisco Router with IVR" chapter.

Ensure that the service provider and region are configured on the Cisco TelePresence Exchange System.

Procedure

To add an IVR resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > IVR Resources**.

The IVR Resources window is displayed.

Step 2 Click **Add A New IVR Resource**.

Step 3 In the entry window that is displayed, enter settings for the IVR Resource.

Table 9-1 describes the entry fields.

Step 4 To save your changes, click **Save**.

Editing IVR Resources

Procedure

To edit an IVR resource, do the following procedure:

Step 1 In the navigation pane, choose **Media Resources > IVR Resources**.

The IVR Resources window is displayed.

Step 2 In the item table, click the applicable entry.

The IVR Resource Details window is displayed.

Step 3 From the toolbar, click **Edit This IVR Resource**.

Step 4 Modify field entries as necessary.

Table 9-1 describes the entry fields.

Step 5 To save your changes, click **Save**.

Deleting IVR Resources

Procedure

To delete an IVR resource, do the following procedure:

Step 1 In the navigation pane, choose **Media Resources > IVR Resources**.

The IVR Resources window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple IVR resources at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of an IVR resource prior to deleting it, in the IVR Resources window, you can click the applicable **IVR Resource** to go to the IVR Resource page. After verifying that you have chosen the correct IVR resource to delete, click **Delete This IVR Resource**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

IVR Resource Fields

Table 9-1 IVR Resource Field Descriptions

Field	Description
Name	Text string identifying this IVR resource. See the "Common Field Properties" section on page 2-4.
Description	Text string describing this IVR resource. See the "Common Field Properties" section on page 2-4.
Region	Drop-down list of the available regions. See the "Adding Regions" section on page 10-5.
Maintenance	Check box. Check the check box to set the IVR resource in a maintenance state.
Host	The IP address (or hostname, if you enable DNS) of the Cisco router.
Port	Enter the port number that is configured on the Cisco router for SIP signaling. The default value of this field is 5060.
Transport Protocol	Drop-down list that specifies the transport protocol between the Cisco TelePresence Exchange System and the IVR resource. Choose **TCP**.

Configuring SIP Resources

The service provider SBC is typically the SIP resource that provides call routing between enterprises and the Cisco TelePresence Exchange System server cluster. The SBC also provides routing between the Cisco TelePresence Exchange System and the remote service providers. You need to configure information about the SBC that is associated with this Cisco TelePresence Exchange System.

The following sections describe how to configure SIP resources:

Adding SIP Resources

Before You Begin

Install and configure the Cisco SBC. For instructions on how to configure a Cisco SBC to interact with the Cisco TelePresence Exchange System, see the "Configuring Cisco Session Border Controllers" chapter.

Configure the service provider and the region on the Cisco TelePresence Exchange System.

Procedure

To add a SIP resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > SIP Resources**.

The SIP Resources window is displayed.

Step 2 Click **Add A New SIP Resource**.

Step 3 In the entry window that is displayed, enter settings for the SIP Resource.

Table 9-2 describes the fields.

Step 4 To save your changes, click **Save**.

Editing SIP Resources

Procedure

To edit a SIP resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > SIP Resources**.

The SIP Resources window is displayed.

Step 2 In the item table, click the applicable entry.

The SIP Resource Details window is displayed.

Step 3 From the toolbar, click **Edit This SIP Resource**.

Step 4 In the window that appears, modify fields as required.

Table 9-2 describes the fields.

Step 5 To save your changes, click **Save**.

Deleting SIP Resources

Procedure

To delete an SIP resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > SIP Resources**.

The SIP Resources window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple SIP resources at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a SIP resource prior to deleting it, in the SIP Resources window, you can click the applicable **SIP Resource** to go to the SIP Resource page. After verifying that you have chosen the correct SIP resource to delete, click **Delete This SIP Resource**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

SIP Resource Fields

Table 9-2 SIP Resource Field Descriptions

Field	Description
Name	Text string identifying this SIP resource. See the "Common Field Properties" section on page 2-4.
Description	Text string describing this SIP resource. See the "Common Field Properties" section on page 2-4.
Region	Drop-down list of the available regions. See the "Adding Regions" section on page 10-5.
Maintenance	Check box. Check the check box to set the SIP resource in a maintenance state.
Host	The IP address (or hostname, if you enable DNS) of the Cisco SBC.
Port	The port number that is configured on the SBC for SIP signaling. The default value of this field is 5060.
Transport Protocol	Drop-down field that specifies the transport protocol between the Cisco TelePresence Exchange System and the SBC. Choose **TCP**.

About Media Resources for Large Meetings

To ensure that media resources are available for large meetings, the Cisco TelePresence Exchange System provides separate media resource pools for large meetings and regular meetings:

- Large meetings include 32 or more segments/ports and are scheduled exclusively on media units that are reserved for large meetings.
- Regular meetings include 31 or fewer segments/ports and are scheduled exclusively on media units that are not reserved for large meetings.

- The system allocates separate resource pools for each media resource type (Cisco TelePresence Multipoint Switch, Cisco TelePresence MCU MSE 8510, and Cisco TelePresence Server MSE 8710). For each media resource type that you provision, you will need to reserve units for large meetings.

Caution To achieve redundancy, you must reserve at least two units (of each resource type) for large meetings and at least two units (of each resource type) for regular meetings.

Configuring CTMS Resources

A Cisco TelePresence Multipoint Switch provides media resources to create multipoint conferences between Cisco TelePresence endpoints. You must configure information about the Cisco TelePresence Multipoint Switch that is associated with this Cisco TelePresence Exchange System.

The following sections describe how to configure CTMS resources:

Adding CTMS Resources

Before You Begin

Install and configure the Cisco TelePresence Multipoint Switch. For instructions on how to configure a Cisco TelePresence Multipoint Switch to interact with the Cisco TelePresence Exchange System, see the "Configuring the Cisco TelePresence Multipoint Switch" chapter.

Configure the resource group that you want to associate with the media resource. For additional information, see the "Configuring Resource Groups" section on page 10-12

Procedure

To add a CTMS resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > CTMS Resources**.

The CTMS Resources window is displayed.

Step 2 Click **Add A New CTMS Resource**.

Step 3 In the entry window that is displayed, enter settings for the CTMS resource.

Table 9-3 describes the fields.

Step 4 To save your changes, click **Save**.

Editing CTMS Resources

Procedure

To edit a CTMS resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > CTMS Resources**.

The CTMS Resources window is displayed.

Step 2 In the item table, click the applicable entry.

The CTMS Resource Details window is displayed.

Step 3 From the toolbar, click **Edit This CTMS Resource**.

Step 4 In the window that is displayed, modify fields as required.

Table 9-3 describes the fields.

Step 5 To save your changes, click **Save**.

Deleting CTMS Resources

Procedure

To delete a CTMS resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > CTMS Resources**.

The CTMS Resources window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple CTMS resources at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a CTMS resource prior to deleting it, in the CTMS Resources window, you can click the applicable **CTMS Resource** to go to the CTMS Resource page. After verifying that you have chosen the correct CTMS resource to delete, click **Delete This CTMS Resource**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Note When a dependency exists, the delete operation aborts and an error message is displayed that describes the dependent configuration item.

CTMS Resource Fields

Table 9-3 CTMS Resource Field Descriptions

Field	Description
Name	Text string to identify the CTMS resource. See the "Common Field Properties" section on page 2-4.
Description	Text string describing the CTMS resource. See the "Common Field Properties" section on page 2-4.
Resource Group	Drop-down list of the available resource groups. See the "Configuring Resource Groups" section on page 10-12.
Maintenance	Check box. Check the check box to set the Cisco TelePresence Multipoint Switch in a maintenance state. The system is not an available resource while in a maintenance state.
Max Capacity	The maximum number of segments that can participate concurrently in a meeting on this Cisco TelePresence Multipoint Switch. The default value is 48 segments.
Host	The IP address (or hostname, if you enable DNS) for the Cisco TelePresence Multipoint Switch. See the "Common Field Properties" section on page 2-4.
Username	Valid user login name for this CTMS resource.
Password	Login password for the above user name.
Port	The port number for Session Initiation Protocol (SIP) signaling. The port number must match the configuration on the Cisco TelePresence Multipoint Switch. The default value is 5060.
Transport Protocol	Drop-down field that specifies the transport protocol between the Cisco TelePresence Exchange System and the Cisco TelePresence Multipoint Switch. Choose **TCP**.
Reserve For Large Meeting	Check box. When you check the check box, you reserve the Cisco TelePresence Multipoint Switch resource for large meetings only. A large meeting includes 32 or more segments/ports. For additional information about the implications of large meetings, see the "About Media Resources for Large Meetings" section on page 9-5.
Vendor Config	A range of static meeting identifiers that are defined on this Cisco TelePresence Multipoint Switch (CTMS). The Cisco TelePresence Exchange uses this information to fulfill requests to join a meeting on this CTMS. For the **Min Static Meeting ID** field, enter the minimum static meeting access number configured for the CTMS. For the **Max Static Meeting ID** field, enter the maximum static meeting access number configured for the CTMS. **Note** To edit this field for an existing resource, the system must be in maintenance mode.

Configuring TPS Resources

The Cisco TelePresence Exchange System interacts with the Cisco TelePresence Server MSE 8710 (TPS) to provide conferences that include multi-screen standards-based endpoints.

Note Before shutting down an active TPS, you must manually set the state of the TPS to maintenance mode through the Cisco TelePresence Exchange System administration console. After the maintenance state is set, the Cisco TelePresence Exchange System reassigns media bridge resources for scheduled meetings that were associated with this TPS to a different TPS within the same resource pool. As part of this transition, dial out calls may be delayed for approximately 3 minutes.

The following sections describe how to configure TPS resources:

Adding TPS Resources

Before You Begin

Install and configure the Cisco TelePresence Server MSE 8710. For instructions on how to configure a Cisco TelePresence Server MSE 8710 to interact with the Cisco TelePresence Exchange System, see the "Configuring Cisco TelePresence MSE 8000 Series" chapter.

Ensure that any previously configured conference IDs are removed before adding the Cisco TelePresence Server MSE 8710 to the Cisco TelePresence Exchange System.

Configure the resource group that you want to associate with the media resource. For additional information, see the "Configuring Resource Groups" section on page 10-12

Procedure

To add a new TPS resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > TPS Resources**.

The TPS Resources window is displayed.

Step 2 Click **Add a New TPS Resource**.

Step 3 In the entry window that is displayed, enter settings for the TPS resource.

Table 9-4 describes the fields.

Step 4 To save your changes, click **Save**.

Editing TPS Resources

Procedure

To edit a Cisco TelePresence Server MSE 8710 resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > TPS Resources**.

The TPS Resources window is displayed.

Step 2 In the item table, click the applicable entry.

The TPS Resource Details window is displayed.

Step 3 From the toolbar, click **Edit This TPS Resource**.

The Edit TPS Resource window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as required.

Fields are described in Table 9-4.

Step 5 To save your changes, click **Save**.

Deleting TPS Resources

Procedure

Step 1 From the navigation pane, choose **Media Resources > TPS Resources**.

The TPS Resources window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple TPS resources at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a TPS resource prior to deleting it, in the TPS Resources window, you can click the applicable **TPS Resource** to go to the TPS Resource page. After verifying that you have chosen the correct TPS resource to delete, click **Delete This TPS Resource**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Note When a dependency exists, the delete operation aborts and an error message is displayed that describes the dependent configuration item.

TPS Resource Fields

Table 9-4 TPS Resource Field Descriptions

Field	Description
Name	Text string identifying the TPS resource. See the "Common Field Properties" section on page 2-4.
Description	Text string describing the TPS resource. See the "Common Field Properties" section on page 2-4.
Resource Group	Drop-down list of the available resource groups. See the "Configuring Resource Groups" section on page 10-12.
Maintenance	Check box. Check the check box to set the Cisco TelePresence Server MSE 8710 in a maintenance state. The system is not an available resource while in a maintenance state.
Max Capacity	The maximum number of segments that can participate concurrently in a meeting on this Cisco TelePresence Server MSE 8710. The default value is 16 segments.
Username	Valid user login name for this Cisco TelePresence Server MSE 8710.
Password	Login password for the above user name.
Host	The IP address (or hostname, if you enable DNS) of the Cisco TelePresence Server MSE 8710. See the "Common Field Properties" section on page 2-4.
Port	The port number for Session Initiation Protocol (SIP) signaling. The port number must match the configuration on the Cisco TelePresence Server MSE 8710. The default value is 5060.
Transport Protocol	Drop-down list that specifies the transport protocol between the Cisco TelePresence Exchange System and the Cisco TelePresence Server MSE 8710. Choose **TCP**.
Reserve For Large Meeting	Check box. Check the check box to reserve the Cisco TelePresence Server MSE 8710 for large meetings. A large meeting includes 32 or more segments/ports. For additional information about the implications of large meetings, see the "About Media Resources for Large Meetings" section on page 9-5.

Table 9-4 TPS Resource Field Descriptions (continued)

Field	Description
Conference Name	Welcome message that is displayed on the TPS screen. The message may contain up to 50 characters. The message may also contain spaces. Cisco recommends that all conference names be the same within a resource group. **Note** You can only edit this field if you are provisioning a new resource or an existing resource. The system must be in maintenance mode.
Vendor Config	Defines a range of permanent meeting identifiers for the Cisco TelePresence Server MSE 8710. The Cisco TelePresence Exchange System uses this information to fulfill requests to join a meeting on this Cisco TelePresence Server MSE 8710 Cisco recommends that you use a four-digit number range for the Cisco TelePresence Server MSE 8710 and Cisco TelePresence MCU MSE 8510 resources, with a range of no more than 100. For example, a range of 7000 to 7100 is acceptable but a range of 7000 to 7150 is not. Integer ranges can be any value between 1 and 2,147,483,647. **Note** The system must be in maintenance mode when editing this field for an existing resource.

Configuring MSE 8510 Resources

The Cisco TelePresence Exchange System interacts with the Cisco TelePresence MCU MSE 8510 (MSE 8510) to provide conferences that can include legacy and third-party single-screen endpoints.

The following sections describe how to configure MSE 8510 resources:

Adding MSE 8510 Resources

Before You Begin

Install and configure the Cisco TelePresence MCU MSE 8510. For instructions on how to configure a Cisco TelePresence MCU MSE 8510 to interact with the Cisco TelePresence Exchange System, see the "Configuring Cisco TelePresence MSE 8000 Series" chapter.

Ensure that any previously configured conference IDs are removed before adding the Cisco TelePresence MCU MSE 8510 to the Cisco TelePresence Exchange System.

Configure the resource group that you want to associate with the media resource. For additional information, see the "Configuring Resource Groups" section on page 10-12.

Procedure

To add a new Cisco TelePresence MCU MSE 8510 resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > MSE 8510 Resources**.

The MSE 8510 Resources window is displayed.

Step 2 Click **Add a New MSE 8510 Resource**.

Step 3 To configure the MSE 8510 resource, enter the settings as indicated in Table 9-5.

Step 4 To save your changes, click **Save**.

Editing MSE 8510 Resources

Procedure

To edit a MSE 8510 resource, do the following procedure:

Step 1 From the navigation pane, choose **Media Resources > MSE 8510 Resources**.

The MSE 8510 Resources window is displayed.

Step 2 In the item table, click the applicable entry.

The MSE 8510 Resource Details window is displayed.

Step 3 From the toolbar, click **Edit This MSE 8510 Resource**.

The Edit MSE 8510 Resource window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as required.

Fields are described in Table 9-5.

Step 5 To save your changes, click **Save**.

Deleting MSE 8510 Resources

Procedure

Step 1 From the navigation pane, choose **Media Resources > MSE 8510 Resources**.

The MSE 8510 Resources window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple MSE 8510 resources at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a MSE 8510 resource prior to deleting it, in the MSE 8510 Resources window, you can click the applicable **MSE 8510 Resource** to go to the MSE 8510 Resource page. After verifying that you have chosen the correct MSE 8510 resource to delete, click **Delete This MSE 8510 Resource**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Note When a dependency exists, the delete operation aborts and an error message is displayed that describes the dependent configuration item.

MSE 8510 Resource Fields

Table 9-5 MSE 8510 Field Descriptions

Field	Description
Name	Text string identifying the MSE 8510 resource. See the "Common Field Properties" section on page 2-4.
Description	Text string describing the MSE 8510 resource. See the "Common Field Properties" section on page 2-4.
Resource Group	Drop-down list of the available resource groups. See the "Configuring Resource Groups" section on page 10-12.
Maintenance	Check box. Check the check box to set the Cisco TelePresence MCU MSE 8510 in a maintenance state. The system is not an available resource while in a maintenance state.
Max Capacity	The maximum number of segments that can participate concurrently in a meeting on this Cisco TelePresence MCU MSE 8510. The default value is 20 segments.
Username	Valid user login name for this Cisco TelePresence MCU MSE 8510.
Password	Login password for the above user name.
Host	The IP address (or hostname, if you enable DNS) of the Cisco TelePresence MCU MSE 8510. See the "Common Field Properties" section on page 2-4.
Port	The port number for Session Initiation Protocol (SIP) signaling. The port number must match the configuration on the Cisco TelePresence MCU MSE 8510. The default value is 5060
Transport Protocol	Drop-down list that specifies the transport protocol between the Cisco TelePresence Exchange System and the Cisco TelePresence MCU MSE 8510. Choose **TCP**.

Table 9-5 MSE 8510 Field Descriptions (continued)

Field	Description
Reserve For Large Meeting	Check box. Check the check box to reserve the Cisco TelePresence MCU MSE 8510 for large meetings. A large meeting includes 32 or more segments/ports. For additional information about the implications of large meetings, see the "About Media Resources for Large Meetings" section on page 9-5.
Vendor Config	Defines a range of permanent meeting identifiers for the Cisco TelePresence MCU MSE 8510. The Cisco TelePresence Exchange System uses this information to fulfill requests to join a meeting on this Cisco TelePresence MCU MSE 8510. Cisco recommends that you use a four-digit number range for the Cisco TelePresence Server MSE 8710 and Cisco TelePresence MCU MSE 8510 resources, with a range of no more than 100. For example, a range of 7000 to 7100 is acceptable but a range of 7000 to 7150 is not. Integer ranges can be any value between 1 and 2,147,483,647. **Note** The system must be in maintenance mode when editing this field for an existing resource.

CHAPTER 10

Configuring Customers

Revised July 3, 2012

The following sections describe how to configure service providers and their customer settings:

Configuring Service Providers

A service provider offers telepresence services to a set of enterprise customers (organizations) by using media resources that are provisioned in one or more regions in the service provider network. Optionally, a service provider can use custom service numbers and Integrated Voice Response (IVR) prompts.

The following sections describe how to configure service providers:

Adding Service Providers

Before You Begin

Configure the help desk route and the corresponding SIP resource.

Procedure

To add a new service provider, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Service Providers**.

The Service Providers window is displayed.

Step 2 From the toolbar, click **Add A New Service Provider**.

Step 3 Enter the fields as appropriate.

Table 10-1 describes the fields.

Step 4 To save your changes, click **Save**.

Editing Service Providers

Procedure

To edit a service provider entry, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Service Providers**.

The Service Providers window is displayed.

Step 2 In the item table, click the applicable entry.

A summary window for the service provider is displayed.

Step 3 From the toolbar, click **Edit This Service Provider**.

The Edit Service Provider window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as appropriate.

Table 10-1 describes the fields.

Step 5 To save your changes, click **Save**.

Deleting Service Providers

Before You Begin

To delete a service provider, you need to remove all of the configuration items that are dependencies of this service provider. The following items might depend on a specific service provider: organizations, service numbers, and resource groups. Other items (such as media resources) might indirectly depend on a specific service provider because they are associated with a resource group.

Note You cannot delete the service provider if a meeting has ever been scheduled for any customer of this service provider.

Procedure

To delete a service provider, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Service Providers**.

The Service Providers window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple service providers at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a service provider prior to deleting it, in the Service Provider window, you can click the applicable **Service Provider** to go to the Service Provider page. After verifying that you have chosen the correct service provider to delete, click **Delete This Service Provider**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Note When a dependency exists, the delete operation aborts and an error message is displayed that describes the dependent configuration item.

Service Provider Fields

Table 10-1 Service Provider Field Descriptions

Field	Description
Name	Text string identifying this service provider. See the "Common Field Properties" section on page 2-4.
Description	Text string describing this service provider. See the "Common Field Properties" section on page 2-4.
Help Desk Number	Digit string. The number to dial to reach the help desk for this service provider. The digit string must be numbers only, and cannot include any spaces, dashes, or characters.
Help Desk Routes	Click **Add Route** to view a drop-down list of available routes. Choose the appropriate route. You can click **Add Route** again to add an alternate route. The route specifies the Session Initiation Protocol (SIP) resource for routing calls to the Help Desk. For more information about routes, see the "Configuring Routes" section on page 12-1.
Default Routes	Click **Add Default Route** to view a drop-down list of available routes. Choose the appropriate route. You can click **Add Default Route** again to add an alternate route. For more information about routes, see the "Configuring Routes" section on page 12-1.
Maximum IVR Queue Time	Maximum length of time in minutes that each guest participant is held in the queue waiting for a host to join. Applicable only when the host and guest roles are enabled for a Meet-Me or Rendezvous meeting. Default time is 10 minutes.

Table 10-1 Service Provider Field Descriptions (continued)

Field	Description
Meeting Extension Enabled By Default	Check box. Check this box to configure the system to automatically extend Meet-Me meetings if resources are available near the end of the meeting. If sufficient resources are available, the meeting continues for a specified length of time. If the extension fails, the system displays the two minute end-of-meeting warning to participants, and ends the meeting after two minutes. **Note** You can configure the Meeting Extension policy at the service provider level, organization level, or meeting level. The policy is hierarchical, so you can configure a meeting to inherit its settings from the meeting scheduler organization. In addition, you can configure an organization to inherit its settings from the service provider. If you want a meeting to inherit organization settings, you must enable the inheritance option at the meeting level. Similarly, if you want an organization to inherit service provider settings, you must enable the inheritance option at the organization level.
Meeting Extension Period (minutes)	*Available only if Meeting Extension Enabled By Default is checked.* Specify the length by which to automatically extend the meeting if resources are available when the meeting nears its configured duration.
Max Meeting Extensions Allowed	*Available only if Meeting Extension Enabled By Default is checked.* Specify the maximum number of times the meeting can be extended if resources are available. **Note** If an administrator or service desk user extends the meeting duration while the meeting is active, the extension counter is reset, and the next extension after the change is counted as the first extension.
Drop Participants on Host Exit in PIN-Enabled Meeting By Default	Check box. Check this check box to configure the system to drop all participants when the host leaves the meeting. If the meeting has more than one host, participants will be dropped when all hosts have left the meeting. This condition is applied to meetings that are configured to inherit host settings from this service provider. **Note** You can configure the host settings at the service provider level, organization level, or meeting level. The policy is hierarchical, so you can configure a Meet-Me or Rendezvous meeting to inherit its settings from the meeting scheduler organization. In addition, you can configure an organization to inherit its settings from the service provider. If you want a meeting to inherit organization settings, you must enable the inheritance option at the meeting level. Similarly, if you want an organization to inherit service provider settings, you must enable the inheritance option at the organization level.

Configuring Regions

A region represents a major geographic region in which a service provider operates. The region contains one or more resource clusters of Cisco TelePresence Multipoint Switches, Cisco TelePresence MSE 8000 Series, Cisco routers with IVR, and session border controllers (SBCs). A resource cluster connects a set of resources within one physical data center. This cluster of resources is also known as a point of presence (POP).

A service provider can configure multiple regions on a Cisco TelePresence Exchange System.

The following sections describe how to configure regions:

Adding Regions

Procedure

To add a new region, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Regions**.

The Regions window is displayed.

Step 2 From the toolbar, click **Add A New Region**.

An entry window is displayed.

Step 3 Enter the appropriate information to configure the region.

Table 10-2 describes the fields.

Step 4 To save your changes, click **Save**.

Editing Regions

Procedure

To edit a region entry, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Regions**.

The Regions window is displayed.

Step 2 In the item table, click the applicable entry.

The Region Details window is displayed.

Step 3 From the toolbar, click **Edit This Region**.

The Edit Region window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as appropriate.

Table 10-2 describes the fields.

Step 5 To save your changes, click **Save**.

Deleting Regions

Before You Begin

To delete a region, you need to remove all of the configuration items (such as resource groups) that are dependencies of this region. For example, remove the region that you want to delete from any associated resource groups.

Note You cannot delete the region if a meeting has ever been scheduled in this region.

Procedure

To delete a region, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Regions**.

The Regions window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple regions at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a region prior to deleting it, in the Regions window, you can click the applicable **Region** to go to the Region page. After verifying that you have chosen the correct region to delete, click **Delete This Region**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Note When a dependency exists, the delete operation aborts, and an error message is displayed that describes the dependent configuration item.

Region Fields

Table 10-2 Region Field Descriptions

Field	Description
Name	Text string identifying this region. See the "Common Field Properties" section on page 2-4.
Description	Text string describing this region. See the "Common Field Properties" section on page 2-4.

Configuring Organizations

An organization is an enterprise customer to which a service provider provides services. An organization controls one or more telepresence endpoints that might be active within a meeting.

The following sections describe how to configure organizations:

Adding Organizations

Before You Begin

Configure the service provider that you want to associate with the organization.

When this organization employs the direct-dial feature, configure the direct dial routes and the corresponding SIP resource.

Procedure

To add a new organization, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Organizations**.

The Organizations window is displayed.

Step 2 From the toolbar, click **Add A New Organization**.

Step 3 Enter the settings as appropriate.

Table 10-3 describes the fields.

Step 4 To save your changes, click **Save**.

Editing Organizations

Procedure

To edit an organization, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Organizations**.

The Organizations window is displayed.

Step 2 In the item table, click the applicable entry.

The Organization Details window is displayed.

Step 3 Click **Edit This Organization**.

The Edit Organization window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as appropriate.

Table 10-3 describes the fields.

Step 5 To save your changes, click **Save**.

Deleting Organizations

Procedure

To delete an organization, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Organizations**.

The Organizations window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple organizations at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of an organization prior to deleting it, in the Organizations window, you can click the applicable **Organization** to go to the Organizations page. After verifying that you have chosen the correct organization to delete, click **Delete This Organization**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Note When a dependency exists, the delete operation aborts, and an error message is displayed that describes the dependent configuration item.

Organization Fields

Table 10-3 Organization Field Descriptions

Field	Description
Name	Text string identifying this organization. See the "Common Field Properties" section on page 2-4.
Description	Text string describing this organization. See the "Common Field Properties" section on page 2-4.
Service Provider	Drop-down list of the available service providers.
Max Ports	Maximum number of ports available to this organization for all concurrent telepresence sessions.
Minimize Capacity	Check the check box to reserve the smallest amount of capacity necessary for an endpoint to attend a meeting. When the check box is not checked, the maximum capacity per endpoint is reserved.
Dial Patterns	Button and drop-down list. Click **Add A Dial Pattern** to display a drop-down list of available dial pattern names. To associate a dial pattern with the organization, choose a dial pattern from the drop-down list. For information on how to configure dial patterns, see the "Configuring Dial Patterns" section on page 12-4 in the "Configuring Call Routing"chapter.
SIP Routes	Button and drop-down list. Click **Add A Route** to display a drop-down list of available SIP routes. For information on how to configure SIP routes, see the "Configuring Routes" section on page 12-1 in the "Configuring Call Routing" chapter. **Note** To route calls, the Cisco TelePresence Exchange System system chooses the first active route configured in this field. If you configure more than one active route, direct dial calls may fail because the first active route may not be the correct route for the call. In this case, the system generates an alarm and does not try to reroute the call. To avoid this type of call failure, we recommend that you make sure the destination endpoint is reachable over all of the configured routes.

Table 10-3 Organization Field Descriptions (continued)

Field	Description
Meeting Extension	Radio buttons provide a choice of the following conditions. The condition is applied to meetings that are configured to inherit Meeting Extension settings from this organization. • Disabled By Default—The system does not automatically extend Meet-Me meetings. • Enabled By Default—The system automatically extends Meet-Me meetings if resources are available near the end of the meeting. If sufficient resources are available, the meeting continues for a specified length of time. If the extension fails, the system displays the two minute end-of-meeting warning to participants, and ends the meeting after two minutes. • Inherit from Service Provider—Use the Meeting Extension settings configured for the service provider. **Note** You can configure the Meeting Extension policy at the service provider level, organization level, or meeting level. The policy is hierarchical, so you can configure a meeting to inherit its settings from the meeting scheduler organization. In addition, you can configure an organization to inherit its settings from the service provider. If you want a meeting to inherit organization settings, you must enable the inheritance option at the meeting level. Similarly, if you want an organization to inherit service provider settings, you must enable the inheritance option at the organization level.
Meeting Extension Period (minutes)	*Available only if Meeting Extension is set to Enabled By Default.* Specify the length by which to automatically extend the meeting if resources are available when the meeting nears its configured duration.
Max Meeting Extensions Allowed	*Available only if Meeting Extension is set to Enabled By Default.* Specify the maximum number of times the meeting can be extended if resources are available. **Note** If an administrator or service desk user extends the meeting duration while the meeting is active, the extension counter is reset, and the next extension after the change is counted as the first extension.

Table 10-3 Organization Field Descriptions (continued)

Field	Description
Drop Participants on Host Exit	Radio buttons provide a choice of the following conditions. The condition is applied to meetings that are configured to inherit host settings from this organization. • Disabled By Default—The system does not drop any participants when the host leaves the meeting. • Enabled By Default—The system drops all participants from the meeting when the host leaves. If the meeting has more than one host, participants will be dropped when all hosts have left the meeting. • Inherit from Service Provider—Use the host settings configured for the service provider. **Note** You can configure the host settings at the service provider level, organization level, or meeting level. The policy is hierarchical, so you can configure a Meet-Me or Rendezvous meeting to inherit its settings from the meeting scheduler organization. In addition, you can configure an organization to inherit its settings from the service provider. If you want a meeting to inherit organization settings, you must enable the inheritance option at the meeting level. Similarly, if you want an organization to inherit service provider settings, you must enable the inheritance option at the organization level.
Allow Inter SP Outgoing Calls	Check box. Check the check box to allow outgoing calls from this organization to other service providers. (This includes calls for Meet-Me and Rendezvous meetings as well as direct-dial calls, because the Cisco TelePresence Exchange System cannot determine the type of an outgoing call.) For Meet-Me and Rendezvous meetings, the policy is enforced between the scheduler organization and the endpoint organization. For direct-dial calls, the policy is enforced between the two endpoints. **Note** If you provide hosted endpoint service and support unprovisioned endpoints, the service provider Cisco Unified Communications Manager must be configured such that each organization uses a single Carrier Information Code (CIC) in order for calls from unprovisioned endpoints to be mapped to the correct organization.
Allow Inter SP Incoming Direct Calls	Check box. Check the check box to allow incoming direct-dial calls to this organization from other service providers. **Note** For unprovisioned endpoints, the Cisco TelePresence Exchange System detects the organization of the endpoint by using the Carrier Identification Code (CIC) code in an incoming INVITE message. The CIC code may be inserted by the Cisco Aggregation Services Router that serves as the Session Border Controller, based on the IP address of the Cisco Unified Communications Manager used by the organization.

Table 10-3 Organization Field Descriptions (continued)

Field	Description
Allow Inter SP Incoming Meet-Me Calls	Check box. Check the check box to allow incoming Meet-Me and Rendezvous meeting calls to this organization from other service providers. **Note** For unprovisioned endpoints, the Cisco TelePresence Exchange System detects the organization of the endpoint by using the Carrier Identification Code (CIC) code in an incoming INVITE message. The CIC code may be inserted by the Cisco Aggregation Services Router that serves as the Session Border Controller, based on the IP address of the Cisco Unified Communications Manager used by the organization.
Enforce Whitelisting	Check box. Check the check box to enforce restrictions on direct-dial calls between this organization and other organizations under the same service provider (also known as intra-SP direct calls). See the "Configuring Whitelist Groups" section on page 10-16 for information on setting up whitelist groups that determine which organizations under the same service provider can dial each other directly. (Meet-Me and Rendezvous meeting calls are always allowed between organizations that belong to the same service provider.)

Configuring Resource Groups

Resource groups provide greater flexibility and control of how media bridge resources are allocated for Meet-Me and Rendezvous meetings. When configuring a resource group, you choose a specific service provider and region and one or more reservation types to be associated with the group. After the resource group has been created, you configure specific media bridge resources to be associated with the group. Based on the set of requirements configured for a meeting (such as service provider, region, reservation type, and endpoint requirements), the system selects the best-fit resource group and associated media bridge resources to use for the meeting.

For information on how to configure reservation types, see the "Configuring Reservation Types" section on page 13-46.

The following sections describe how to configure resource groups:

Adding Resource Groups

Before You Begin

Configure the service provider, region, and reservation types that you want to associate with the resource group.

Procedure

To add a new resource group, do the following procedure:

Step 1 From the navigation pane, choose **Customers** > **Resource Groups**.

The Resource Groups window is displayed.

Step 2 From the toolbar, click **Add A New Resource Group**.

Step 3 Enter the fields as appropriate.

Table 10-4 describes the fields.

Step 4 To save your changes, click **Save**.

Editing Resource Groups

Procedure

To edit a resource group, do the following procedure:

Step 1 From the navigation pane, choose **Customers** > **Resource Groups**.

The Resource Groups window is displayed.

Step 2 In the item table, click the applicable entry.

A summary window for the resource group is displayed.

Step 3 From the toolbar, click **Edit This Resource Group**.

The Edit Resource Group window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as appropriate.

Table 10-4 describes the fields.

Step 5 To save your changes, click **Save**.

Viewing Resource Group Details

Procedure

To view a summary of the reservation types or media resources assigned to a resource group, do the following procedure:

Step 1 From the navigation pane, choose **Customers** > **Resource Groups**.

The Resource Groups window is displayed.

Step 2 In the item table, click the applicable entry.

A summary window for the resource group is displayed.

Step 3 To view a summary of the reservation types, Cisco TelePresence Multipoint Switch (CTMS) resources, Cisco TelePresence MCU MSE 8510 (MSE 8510) resources, or Cisco TelePresence Server MSE 8710 (TPS) Resources assigned to this resource group, click **Reservation Types**, **CTMS Resources**, **MSE 8510 Resources**, or **TPS Resources**.

A summary window is displayed.

Note In the summary window for the reservation types, the Total Ports column represents the total ports available for meeting reservations across all media resources (CTMS, MSE 8510, and TPS resources assigned to large or regular meetings) within this resource group.

Deleting Resource Groups

Before You Begin

To delete a resource group, you need to remove all of the configuration items (such as media resources) that are dependencies of this resource group. For example, remove the resource group that you want to delete from any associated media resources.

Procedure

To delete a resource group, do the following procedure:

Step 1 From the navigation pane, choose **Customers** > **Resource Groups**.

The Resource Groups window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple resource groups at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a resource group prior to deleting it, in the Resource Group window, you can click the applicable resource group to go to the Resource Group page. After verifying that you have chosen the correct resource group to delete, click **Delete This Resource Group** in the toolbar, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Note When a dependency exists, the delete operation aborts and an error message is displayed that describes the dependent configuration item.

Resource Group Fields

Table 10-4 Resource Group Field Descriptions

Field	Description
Name	Text string identifying this resource group. See the "Common Field Properties" section on page 2-4.
Description	Text string describing this resource group. See the "Common Field Properties" section on page 2-4.
Region	Drop-down list of the available regions.
Service Provider	Drop-down list of the available service providers.
Overflow	Calculated value (percentage): 100% - (Sum of the Dedication Percentages for all specified reservation type names within the resource group) = Overflow The overflow percentage represents the percentage of the total media bridge resources within the resource group that is not assigned to a specific reservation type. When a resource group runs out of dedicated resources, the system will use the overflow to allocate a resource for a guaranteed meeting only, not a best-effort meeting. The system restricts the use of overflow to only the time when a resource is actually being allocated for a meeting. The system will not use the overflow at the time when you create a meeting. **Note** Cisco recommends an overflow value of 20%.
Reservation Type Name	Click **Add Reservation Type** to view a drop-down list of available reservation types. Choose the appropriate reservation type name. You can click **Add Reservation Type** again to add more reservation types.

Table 10-4 Resource Group Field Descriptions (continued)

Field	Description
Dedication Percentage	Percentage of the total media bridge resources within a resource group that is reserved for the specified reservation type name. The dedication percentage can be distributed over two or more reservation types. A warning message will be displayed if the sum of the dedication percentages for all specified reservation types within the resource group exceeds 100%. If this sum is less than 100%, the remaining percentage is assigned as overflow resources. **Note** Cisco recommends that you avoid decreasing dedication percentage values after any resources contained within the resource group have been reserved for meetings. Decreasing the dedication percentage may cause these meetings to fail.
Booking Percentage	Percentage of the dedicated media bridge resources within a resource group that you can use to create meetings for the specified reservation type name. If you try to set the booking percentage less than 100%, a warning message will be displayed. For guaranteed meetings, the system sets the booking percentage to 100% to ensure that enough media bridge resources are reserved for the meeting. For best-effort meetings, set the booking percentage greater than 100% to allow for overbooking of the media bridge resources. For example, a booking percentage of 150% allows you to reserve 50% more media bridge resources than the dedicated amount. Overbooking assumes that all Meet-Me and Rendezvous meetings associated with a specific reservation type will not be active at the same time.

Configuring Whitelist Groups

Whitelist groups enable you to define policies that control direct-dialed calls between organizations associated with a single service provider (also known as intra-service provider calls). The policies apply to both provisioned and unprovisioned endpoints.

A whitelist group can contain more than one organization, and an organization can belong to more than one whitelist group. If two organizations are members of the same whitelist group, direct-dial calls between the organizations are allowed. If the organizations are not members of the same whitelist group, direct-dial calls between the organizations are rejected. The Cisco TelePresence Exchange System call detail records (CDRs) identify calls that are rejected due to a whitelist policy restriction.

Note In order for whitelist groups to be applied between two organizations, the Enforce Whitelisting check box must be checked on at least one of the organizations.

The following sections describe how to configure whitelists:

- Adding Whitelist Groups, page 10-17
- Editing Whitelist Groups, page 10-17
- Deleting Whitelist Groups, page 10-18

- Whitelist Group Fields, page 10-18

Adding Whitelist Groups

Before You Begin

Configure the organizations that you want to associate with the whitelist group. Check the Enforce Whitelisting check box for each organization for which you want to restrict outgoing and incoming intra-service provider calls.

Note If you provide hosted endpoint service and support unprovisioned endpoints, the service provider Cisco Unified Communications Manager must be configured such that each organization uses a single Carrier Information Code (CIC) in order for calls from unprovisioned endpoints to be mapped to the correct organization.

Procedure

To add a new whitelist, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Whitelist Groups**.

The Whitelist Groups window is displayed.

Step 2 From the toolbar, click **Add A New Whitelist Group**.

Step 3 Enter the settings as appropriate.

Table 10-5 describes the fields.

Step 4 To save your changes, click **Save**.

Editing Whitelist Groups

Procedure

To edit a whitelist group, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Whitelist Groups**.

The Whitelist Groups window is displayed.

Step 2 In the item table, click the applicable entry.

The Whitelist Group Details window is displayed.

Step 3 Click **Edit This Whitelist Group**.

The Edit Whitelist Group window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as appropriate.

Table 10-5 describes the fields.

Step 5 To save your changes, click **Save**.

Deleting Whitelist Groups

Procedure

To delete a whitelist group, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Whitelist Groups**.

The Whitelist Groups window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple whitelist groups at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a whitelist group prior to deleting it, in the Whitelist Groups window, you can click the applicable **Whitelist Group** to go to the Whitelist Group page. After verifying that you have chosen the correct group to delete, click **Delete This Whitelist Group**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Whitelist Group Fields

Table 10-5 Whitelist Group Field Descriptions

Field	Description
Name	Text string identifying this whitelist group. See the "Common Field Properties" section on page 2-4.
Service Provider	Drop-down list of the available service providers. Choose the service provider to which this whitelist group applies. For more information about service providers, see the "Configuring Service Providers" section on page 10-1.
Organizations	Organizations that belong to the same whitelist group can dial each other directly. (Meet-Me and Rendezvous meeting calls are always allowed between organizations that belong to the same service provider.) Direct-dial calls are blocked between organizations that do not appear together in any whitelist group, as long as the Enforce Whitelisting check box is checked for either organization. Click **Add An Organization** to display a drop-down list of organizations that are associated with the selected service provider, and choose an organization to add to the whitelist group. For more information about organizations, see the "Configuring Organizations" section on page 10-7.

CHAPTER 11

Configuring Endpoints

The following sections describe how to configure endpoints:

Configuring Endpoints

The Cisco TelePresence Exchange System supports three types of endpoints:

- Provisioned endpoints—Endpoints for which all configuration details (such as name, phone number, number of screens, and organization) are known by the administrator and configured on the Cisco TelePresence Exchange System. If an organization has chosen hosted endpoint service, the endpoints are provisioned endpoints.
- Unprovisioned endpoints—Endpoints for which limited configuration details are known by the administrator. Through the administration console, you can add unprovisioned endpoints to participate in meetings hosted by the Cisco TelePresence Exchange System.
- Remote endpoints—Endpoints for which none of the configuration details are known by the administrator. Remote endpoints are endpoints that join the meeting from another service provider network. Through the administration console, you can add remote endpoints to participate in meetings hosted by the Cisco TelePresence Exchange System.

The following sections describe how to configure endpoints:

Adding Endpoints

Before You Begin

Configure the organization that hosts the endpoint.

Procedure

To add a new endpoint, do the following procedure:

Step 1 From the navigation pane, choose **Endpoint Management** > **Endpoints**.

The Endpoints window is displayed.

Step 2 From the toolbar, click **Add a New Endpoint**.

Step 3 Enter the settings as indicated in Table 11-1 to configure the endpoint.

Step 4 To save your changes, click **Save**.

Editing Endpoints

Procedure

To edit an endpoint, do the following procedure:

Step 1 From the navigation pane, choose **Endpoint Management** > **Endpoints**.

The Endpoints window is displayed.

Step 2 In the item table, click the applicable entry.

Details for the endpoint are displayed.

Tip To see a list of all the past and future meetings to which the endpoint has been invited, click the Meetings tab.

Step 3 From the toolbar, click **Edit This Endpoint**.

The Edit Endpoint window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as required.

Table 11-1 describes the fields.

Step 5 To save your changes, click **Save**.

Migrating Endpoints

The Migrate Endpoints window enables you to change the media profile configuration of one or more endpoints that belong to the same organization at the same time.

Procedure

To change the media profile configuration of one or more endpoints, do the following procedure.

Step 1 From the navigation pane, choose **Endpoint Management** > **Endpoints**.

The Endpoints window is displayed.

Step 2 From the toolbar, click **Migrate Endpoints**.

Step 3 Select a Migration Type:

- **Native Interop Migration**—All existing endpoints in the organization that are configured with a built-in (predefined) CTS media profile will be migrated to the (Native Interop) version of the media profile. For example, endpoints with the CTS-3200 media profile will be migrated to the CTS-3200 (Native Interop) media profile.

  Note The Native Interop profiles require specific software versions on the CTS and bridge. See the "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection" appendix for more information.

- **Custom Migration**—Each endpoint in the organization that is configured with a particular media profile will be migrated to a new media profile that you specify.

Step 4 From the Organization drop-down list, choose the organization to which the endpoints to be migrated belong.

Step 5 If you selected **Custom Migration** in Step 3, choose the media profile to be migrated, and the new media profile.

Step 6 To see a list of the endpoints that will be migrated, click **Preview Endpoints**.

The endpoints to be migrated are displayed at the bottom of the window, along with the current and new media profile for each.

Step 7 Click **Migrate Endpoints**. The number of endpoints that were migrated is displayed at the top of the window.

Deleting Endpoints

Procedure

To delete an endpoint, do the following procedure:

Note In order to delete an endpoint, you must first delete all associated meetings, including both past and future meetings. The procedure includes steps to locate and delete associated meetings.

Step 1 From the navigation pane, choose **Endpoint Management > Endpoints**.

The Endpoint window is displayed.

Step 2 To delete one or more endpoints that may have past or future meetings associated with them, skip to Step 3. To delete multiple endpoints that do not have past or future meetings associated with them, do the following substeps:

a. In the item table, check the check box next to the entry that you want to delete. You can delete multiple endpoints at one time by checking the check box next to each entry that you want to delete.

b. Click **Delete**.

c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Step 3 To delete all meetings associated with an endpoint and then delete an endpoint, do the following substeps:

a. In the Endpoints window, click the applicable **Endpoint** to go to the Endpoint page.

b. Click the **Meetings** tab. The list of meetings associated with the endpoint displays.

c. In the item table, check the check box next to each meeting (or check the check box at the top of the table to select all rows), then click **Delete**.

d. Click **Delete This Endpoint**.

e. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Step 4 Repeat Step 3 for each additional endpoint that you plan to delete.

Endpoints Fields

Table 11-1 Endpoint Field Descriptions

Field	Description
Name	Text string to identify this endpoint. See the "Common Field Properties" section on page 2-4.
Description	Text string to describe the endpoint. See the "Common Field Properties" section on page 2-4.
Number	E.164 number or the username part of the SIP URI (the characters that precede the @ symbol in the SIP URI). **Note** There is no need to note a country code in the number. **Note** For dial out calls made from the Cisco TelePresence Exchange System to provisioned endpoints that are registered with a Cisco VCS using a SIP URI, you must add a transform rule on the Cisco VCS. For more information, see the "Configuring Cisco VCS Settings" section in the "Configuring Cisco TelePresence MSE 8000 Series"chapter.
Active	Check box. If you check the Active check box, the endpoint becomes available immediately.
Organization	Drop-down list of available organizations. Choose the organization that hosts the endpoint.
Media Profile	Drop-down list of endpoint types. Choose the media type that corresponds to the endpoint.
Supports OBTP	Check box. Check this check box for provisioned endpoints in order to support One-Button-to-Push (OBTP) functionality.

Table 11-1 Endpoint Field Descriptions (continued)

Field	Description
CTS-MAN	(Optional) Is displayed when you check the Support OBTP check box. Drop-down list of available Cisco TelePresence Managers. Choose the Cisco TelePresence Manager that connects with the Cisco Unified Communications Manager (Unified CM) that hosts this endpoint. **Note** For more details on the Unified CM settings set on the Cisco TelePresence Manager, see the "Configuring Cisco Unified Communications Manager" chapter. This field is required only for endpoints that support OBTP.
Hosted Room	(Optional) Is displayed when you check the Support OBTP check box. Drop-down list of hosted rooms available on the Cisco TelePresence Manager. Choose the room that corresponds to this endpoint. **Note** The Cisco TelePresence Manager automatically refreshes the hosted room listing every hour. To update the room listing in between the hourly updates, click **Refresh Room List**.

Configuring Media Profiles

You must assign a media profile for each type of endpoint that connects to this Cisco TelePresence Exchange System.

The media profile contains information that allows different types of endpoints to connect successfully.

Built-in (pre-defined) media profiles exist for Cisco endpoints. Most non-Cisco endpoints can use the Generic H.323 or Generic SIP built-in media profiles. When you are adding a non-Cisco endpoint, Cisco recommends creating a specific media profile for that endpoint.

The following sections describe how to configure media profiles:

Adding Media Profiles

Procedure

To add a new media profile, do the following procedure:

Step 1 From the navigation pane, choose **Endpoint Management** > **Media Profiles**.

The Media Profiles window is displayed.

Step 2 Click **Add a New Media Profile**.

Step 3 Enter the settings as appropriate.

Table 11-2 describes the settings for the media profile.

Step 4 To save your changes, click **Save**.

Editing Media Profiles

Note You cannot edit the built-in media profiles.

Procedure

To edit a media profile, do the following procedure:

Step 1 From the navigation pane, choose **Endpoint Management** > **Media Profiles**.

The Media Profiles window is displayed.

Step 2 In the item table, click the applicable entry.

The Media Profile Details window is displayed.

Step 3 From the toolbar, click **Edit This Media Profile**.

The Edit Media Profile window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as required.

Table 11-2 describes the fields.

Step 5 To save your changes, click **Save**.

Deleting Media Profiles

Note You cannot delete the built-in media profiles.

Procedure

To delete a media profile, do the following procedure:

Step 1 From the navigation pane, choose **Endpoint Management** > **Media Profiles**.

The Media Profiles window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple media profiles at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a media profile prior to deleting it, in the Media Profiles window, you can click the applicable **Media Profile** to go to the Media Profile page. After verifying that you have chosen the correct media profile to delete, click **Delete This Media Profile**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Media Profile Fields

Table 11-2 Media Profile Field Descriptions

Field	Description
Name	Text string to identify this media profile. See the "Common Field Properties" section on page 2-4.
Description	Text string to describe the media profile. See the "Common Field Properties" section on page 2-4.
Number of Screens	Numeric value. Enter the number of screens (segments) that this endpoint type provides.
Protocols	Check boxes. Choose the media protocol(s) supported by this endpoint type. The choices include ISDN, H323, SIP, TIP and MUX.
Built In	(Read-Only Field) Boolean. The system automatically assigns the read-only field value after the configuration of the media profile is complete, and displays it on the Media Profiles Summary window. Field is set to TRUE for each default media profile and is set to FALSE for any media profiles that you add.
Manufacturer	(Optional) Text string. Enter the manufacturer. This field is for information only.
Supports 30 FPS Presentation	Check box. Check the box if the endpoint type has a presentation codec that supports 30 frames per second for graphics collaboration.

Configuring CTS Manager Resources

The Cisco TelePresence Exchange System communicates with the Cisco TelePresence Manager to obtain information about the telepresence endpoints that are associated with hosted subscribers.

You need to configure information about the Cisco TelePresence Manager that is associated with this Cisco TelePresence Exchange System.

The following sections describe how to configure CTS Manager resources:

Adding CTS Manager Resources

Before You Begin

Install and configure the Cisco TelePresence Manager. For additional information, see the "Configuring Cisco TelePresence Manager" chapter.

You need a valid login ID and password for the Cisco TelePresence Manager to configure it on the Cisco TelePresence Exchange System.

Procedure

To add a new Cisco TelePresence Manager resource, do the following procedure:

Step 1 From the navigation pane, choose **Endpoint Management > CTS-MAN Resources**.

The CTS-MAN Resources window is displayed.

Step 2 From the toolbar, click **Add a New CTS-MAN Resource**.

Step 3 Enter settings as appropriate.

Table 11-3 summarizes the field descriptions for the Cisco TelePresence Manager resource.

Step 4 Click **Test Connection** to verify the connection between the Cisco TelePresence Exchange System and Cisco TelePresence Manager.

Step 5 To save your changes, click **Save**.

Editing CTS Manager Resources

Procedure

To edit a Cisco TelePresence Manager resource, do the following procedure:

Step 1 From the navigation pane, choose **Endpoint Management > CTS-MAN Resources**.

The CTS-MAN Resources window is displayed.

Step 2 In the summary list, click the applicable entry.

Details for the resource display.

Step 3 From the toolbar, click **Edit This CTS-MAN Resource**.

The Edit CTS-MAN Resource window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as necessary.

Table 11-3 summarizes the field descriptions.

Step 5 To save your changes, click **Save**.

Deleting CTS Manager Resources

Before You Begin

Note the following before deleting the Cisco TelePresence Manager resource.

When you delete a Cisco TelePresence Manager resource, all endpoints that are associated with the deleted resource and that previously were configured to support OBTP, lose the ability to support OBTP.

A review of the endpoint configuration window for affected endpoints (**Endpoint Management > Endpoints >** *Endpoint*) shows that the check box **Support OBTP** is no longer checked. However, all other configuration parameters for those endpoints remain intact on the Cisco TelePresence Exchange System.

After you delete the Cisco TelePresence Manager resource, you can edit the configuration for those affected endpoints to again allow support for OBTP. After this configuration is done, the system locates and assigns a new Cisco TelePresence Manager.

Procedure

To delete a Cisco TelePresence Manager resource, do the following procedure:

Step 1 From the navigation pane, choose **Endpoint Management > CTS-MAN Resources**.

The CTS-MAN Resources window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple Cisco TelePresence Manager resources at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a Cisco TelePresence Manager resource prior to deleting it, in the CTS-MAN Resources window, you can click the applicable **CTS-MAN Resource** to go to the CTS-MAN Resource page. After verifying that you have chosen the correct Cisco TelePresence Manager resource to delete, click **Delete This CTS-MAN Resource**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

CTS Manager Fields

Table 11-3 CTS Manager Field Descriptions

Field	Description
Name	Text string identifying the Cisco TelePresence Manager. See the "Common Field Properties" section on page 2-4.
Description	Text string describing the Cisco TelePresence Manager. See the "Common Field Properties" section on page 2-4.

Table 11-3 CTS Manager Field Descriptions (continued)

Field	Description
Maintenance Mode	Check box. Check the check box to set the Cisco TelePresence Manager in a maintenance state. The CTS-MAN must be in maintenance mode in order for you to edit the Host, Username, or Password fields.
Host	The IP address of the Cisco TelePresence Manager. See the "Common Field Properties" section on page 2-4.
Username	Valid user login name for this Cisco TelePresence Manager.
Password	Login password for the above user name.

CHAPTER 12

Configuring Call Routing

The following sections describe how to configure call routing by using the administrative console:

Configuring Routes

To route direct dial and SIP dial out calls, the Cisco TelePresence Exchange System first needs to identify the organization or remote service provider for which the call is intended. The system can identify a destination organization if the dial pattern of the call exactly matches the number of a provisioned endpoint. If the dial pattern does not match the number of a provisioned endpoint, the system systematically tries to match the dial pattern of the call with the dial patterns configured on the system for remote service providers and then organizations. If a match is found, the system identifies the associated organization or remote service provider as the destination for the call. If no match is found, the system sends the call to a default route. If you have not configured an active default route, then the system rejects the call. For information about dial patterns, see the "Configuring Dial Patterns" section on page 12-4.

After the system identifies the destination organization or remote service provider, the system finds the first active route associated with the destination for the call. The route provides a pointer to a resource. The system then forwards the call to the resource associated with the active route. The route also provides a unique tag value that is added to the outgoing SIP message.

In most cases, the resource associated with the active route is a Session Border Controller (SBC). When configured properly, each adjacency on the SBC is also assigned a unique tag value. When the SBC receives a SIP message from the Cisco TelePresence Exchange System, the SBC routes the call to the adjacency whose tag matches the tag on the message.

The following sections describe how to configure SIP routes. After you configure a route, you can associate the route with a specific service provider, organization, or remote service provider. For information about how to associate a route with a service provider or organization, see the "Configuring Customers" chapter. For information about how to associate a route with a remote service provider, see the "Configuring Remote Service Providers" section on page 12-7.

Adding Routes

Before You Begin

Configure SIP resources.

Procedure

To add a new route, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > Routes**.

The Routes window is displayed.

Step 2 Click **Add A New Route**.

Step 3 Enter the settings as indicated in Table 12-1 to configure the route.

Step 4 To save your changes, click **Save**.

Editing Routes

Procedure

To edit a route, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > Routes**.

The Routes window is displayed.

Step 2 In the item table, click the applicable entry.

The Route Details window is displayed.

Step 3 From the toolbar, click **Edit This Route**.

The Edit Route window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as required.

Fields are described in Table 12-1.

Step 5 To save your changes, click **Save**.

Deleting Routes

Procedure

To delete a route, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > Routes**.

The Routes window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple routes at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a route prior to deleting it, in the Routes window, you can click the applicable **Route** to go to the Routes page. After verifying that you have chosen the correct route to delete, click **Delete This Route**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Route Fields

Table 12-1 Route Field Descriptions

Field	Description
Name	Text string to identify this route. See the "Common Field Properties" section on page 2-4.
Description	Text string describing this route. See the "Common Field Properties" section on page 2-4.
SIP Resource	Drop-down list. Choose the SIP resource for this route. The SIP resource is generally a session border controller (SBC) that provides call routing between enterprises and the Cisco TelePresence Exchange System server cluster. The SBC also provides routing between the Cisco TelePresence Exchange System and remote service providers. See the "Adding SIP Resources" section on page 9-4.
SIP Tag	The SBC tag for this route. This value must match the tag that the SBC assigns to the associated adjacency. The tag value must be unique in this Cisco TelePresence Exchange System.
Route Type	Drop-down list. Choose either INCOMING, OUTGOING, or BOTH. This value controls the direction for which the call is intended on this route. If you cannot specify separate routes for incoming and outgoing calls, choose BOTH.

Table 12-1 Route Field Descriptions (continued)

Field	Description
Endpoint Type	Drop-down list. Choose one of the following values: • CTS—Indicates that the endpoints served by this route are all TIP-based Cisco TelePresence System endpoints. • Interop—Indicates that none of the endpoints served by this route are TIP-based Cisco TelePresence System endpoints. • Both—Indicates that a mixture of endpoints are served by this route. Choose this value if unprovisioned endpoints are served by this route. **Caution** If you select **Interop** or **Both**, any incoming calls from a TIP-based Cisco Telepresence System endpoint to a conference that is hosted on a Cisco TelePresence Server MSE 8710 (TPS) will fail. Therefore, if calls over this route must be able to connect to a TPS, select only the **CTS** value in this field.
Active	Check box. Check this check box to allow the Cisco TelePresence Exchange System to send calls to this route. If this check box is not checked, the Cisco TelePresence Exchange System will not send calls to this route.

Configuring Dial Patterns

For direct dial and SIP dial out calls, the Cisco TelePresence Exchange System provides call routing capabilities that are based on matching (specifying and recognizing) strings of text called dial patterns. You can specify the rule for dial pattern matching to be based on either a number or domain (the characters that follow the @ symbol in the SIP URI) and then associate the rule to a destination organization or remote service provider.

If the dial pattern rule is specified for a destination number, you can further configure the dial pattern rule to exactly match the dial pattern of the destination number or to match only the prefix, suffix, or regular expression of the destination number. If the dial pattern rule is specified for a destination domain, you can only configure the dial pattern rule to exactly match the characters that follow the @ symbol in the SIP URI.

The following sections describe how to configure dial patterns. After you configure a dial pattern, you can associate the dial pattern with a specific organization or remote service provider. For information about how to associated a dial pattern with an organization, see the "Configuring Organizations" section in the "Configuring Customers" chapter. For information about how to associate a dial pattern with a remote service provider, see the "Configuring Remote Service Providers" section on page 12-7.

Adding Dial Patterns

Procedure

To add a new dial pattern, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > Dial Patterns**.

The Dial Patterns window is displayed.

Step 2 Click **Add A New Dial Pattern**.

Step 3 Enter the settings as indicated in Table 12-2 to configure the dial pattern.

Step 4 To save your changes, click **Save**.

Editing Dial Patterns

Procedure

To edit a dial pattern, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > Dial Patterns**.

The Dial Patterns window is displayed.

Step 2 In the item table, click the applicable entry.

The Dial Pattern Details window is displayed.

Step 3 From the toolbar, click **Edit This Dial Pattern**.

The Edit Dial Pattern window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as required.

Fields are described in Table 12-2.

Step 5 To save your changes, click **Save**.

Deleting Dial Patterns

Procedure

To delete a dial pattern, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > Dial Patterns**.

The Dial Patterns window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple dial patterns at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a dial pattern prior to deleting it, in the Dial Patterns window, you can click the applicable **Dial Pattern** to go to the Dial Patterns page. After verifying that you have chosen the correct dial pattern to delete, click **Delete This Dial Pattern**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Dial Patterns Fields

Table 12-2 Dial Pattern Field Descriptions

Field	Description
Name	Text string to identify the dial pattern. See the "Common Field Properties" section on page 2-4.
Description	Text string describing the dial pattern. See the "Common Field Properties" section on page 2-4.
Pattern Part	Drop-down list. The pattern part specifies which portion of the pattern definition the Cisco TelePresence Exchange System uses to match the dial pattern. You indicate the pattern definition in the Pattern field. The available pattern parts are as follows: • Number—Matches the number part of the pattern based on type specified in the Pattern Type field. • Domain—Uses the exact characters defined in the Pattern field to match the characters that follow the @ symbol in the SIP URI. **Note** If you select the Domain pattern part option, the Cisco TelePresence Exchange System supports only the Exact pattern type option.

Table 12-2 Dial Pattern Field Descriptions (continued)

Field	Description
Pattern Type	Drop-down list. The pattern type specifies how the Cisco TelePresence Exchange System uses the pattern definition to match the dial pattern. You indicate the pattern definition in the Pattern field. The available pattern types are as follows: • Exact—If you specified the Number pattern part, match by using the exact number that is entered in the pattern. If you specified the Domain pattern part, match by using the exact characters entered in the pattern. • Prefix—Match by using the prefix in the pattern. • Suffix—Match by using the suffix in the pattern. • Regex—Match by using the regular expression in the pattern. The Cisco TelePresence Exchange System enforces the following rule of precedence when trying to find a dial pattern match: 1. Exact domain 2. Exact number 3. Prefix number 4. Suffix number 5. Regex number
Pattern	The definition of the pattern. The format of the pattern depends on the option specified in the Pattern Part field. If you specified the Number pattern part, the pattern must be a number consisting of E.164 numbers. If you specified the Domain pattern part, the pattern must be a domain consisting of alphanumeric characters, hyphens, and dots.

Configuring Remote Service Providers

Customers can attend meetings hosted by a remote service provider. To attend the meeting, the user dials a number that matches the dial pattern that is associated with the remote service provider. The Cisco TelePresence Exchange System routes the user request to an SBC that establishes communication with the remote service provider.

The following sections describe how to configure remote service providers:

- Adding Remote Service Providers, page 12-8
- Editing Remote Service Providers, page 12-8
- Deleting Remote Service Providers, page 12-8
- Remote Service Provider Fields, page 12-9

Adding Remote Service Providers

Procedure

To add a new remote service provider, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > Remote Service Providers**.

The Remote Service Providers window is displayed.

Step 2 Click **Add A New Remote Service Provider**.

Step 3 Enter the settings as indicated in Table 12-3 to configure the remote service provider.

Step 4 To save your changes, click **Save**.

Editing Remote Service Providers

Procedure

To edit a remote service provider, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > Remote Service Providers**.

The Remote Service Providers window is displayed.

Step 2 In the item table, click the applicable entry.

The Remote Service Provider Details window is displayed.

Step 3 From the toolbar, click **Edit This Remote Service Provider**.

The Edit Remote Service Provider window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as required.

Fields are described in Table 12-3.

Step 5 To save your changes, click **Save**.

Deleting Remote Service Providers

Procedure

To delete a remote service provider, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > Remote Service Providers**.

The Remote Service Providers window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple remote service providers at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a remote service provider prior to deleting it, in the Remote Service Providers window, you can click the applicable **Remote Service Provider** to go to the Remote Service Providers page. After verifying that you have chosen the correct remote service provider to delete, click **Delete This Remote Service Provider**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Remote Service Provider Fields

Table 12-3 Remote Service Provider Field Descriptions

Field	Description
Name	Text string to identify the remote service provider. See the "Common Field Properties" section on page 2-4. **Note** For clear reporting in the call detail records, the remote service provider name should be unique. Choose a name that does not match the name of any other service provider or remote service provider that is configured in the system.
Description	Text string describing the remote service provider. See the "Common Field Properties" section on page 2-4.
Dial Patterns	Button and drop-down list. Click **Add A Dial Pattern** to display a drop-down list of available dial pattern names. To associate a dial pattern with the remote service provider, choose a dial pattern from the drop-down list. You can add multiple dial patterns by repeating the above procedure. For information on how to configure dial patterns, see the "Configuring Dial Patterns" section on page 12-4.
SIP Routes	Button and drop-down list. Click **Add A Route** to display a drop-down list. To associate a SIP route with the remote service provider, choose a route from the drop-down list. **Note** SBCs manage call routing between the Cisco TelePresence Exchange System and remote service providers. You can add multiple routes, ordered by priority, to accommodate SBC fail over. To add multiple routes, click **Add A Route** and choose another route from the drop-down list. Repeat this procedure for each route. For information about routes, see the "Adding Routes" section on page 12-2.

Viewing Call Detail Records

The Cisco TelePresence Exchange System collects and displays call detail records (CDRs) for calls that are placed on the system. From the administration console, you can view CDR details for the system as well as export a comma separated value (.csv) file of that information.

The Cisco TelePresence Exchange System retains CDRs for up to 30 days from the recorded end time of the CDR. The system automatically purges CDRs that exceed this 30-day limit. If the total number of CDRs retained by the system reaches 100,000, the system retains only the most recent 100,000 records and automatically purges the rest.

When viewing CDRs through the administration console, you can filter the listing by each category heading (such as caller, service provider, organization, Meet-Me conference ID, and start and end time).

The following sections describe how to view, export, and filter CDRs:

- Viewing and Filtering CDRs, page 12-10
- Exporting a CDR File, page 12-11
- CDR Fields, page 12-11

For instructions on viewing intra-company call detail records, see the "Viewing Intra-Company CDRs" section on page 12-16.

Viewing and Filtering CDRs

Procedure

To view and filter CDRs for the system, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > CDRs**.

The CDRs window is displayed showing details on meetings for the past 30 days. Fields are described in Table 12-4.

Step 2 (Optional) To filter the information that is displayed on the CDRs window, do one of the following:

- To filter on the call type and CDR source information that is displayed on the CDR window, click the **T** icon next to the column heading, and check the check boxes next to each item that you want to display on the window.

  To display CDRs for all items, check **All**.
- To filter on any specific heading other than call type and CDR source such as organization (for example ABC Company), click the **T** icon next to the column heading, and enter the specific item on which you want to filter.

Step 3 To activate the filter, click **Filter**.

To deactivate a filter, click the **T** icon next to the appropriate column heading and click **Clear**.

Note When you click **Clear Filters**, the system clears all defined filters.

Exporting a CDR File

To capture the information that is displayed on the **Call Routing > CDRs** window, you can export a CDR file. When you export the CDR file, additional information for each CDR entry is available beyond what is viewable on the CDRs window, for example, the call engine name and IP address, which can be useful for troubleshooting purposes.

Procedure

To export a CDR file from the system, do the following procedure:

Step 1 From the navigation pane, choose **Call Routing > CDRs**.

The CDRs window is displayed showing details on meetings.

Step 2 To export a file that summarizes CDRs for the last 30 days, click **Export CDRs**.

A panel appears with options to either view or save the export.csv file. Fields are described in Table 12-5.

CDR Fields

Table 12-4 CDR Field Descriptions for Fields Displayed on the CDRs Window

Field	Description
Caller	The value of the Caller field is dependent on the Call Type as follows: • DIRECTDIAL—E.164 number or the username part of the SIP URI (the characters that precede the @ symbol in the SIP URI) of the calling endpoint (caller). • MEETME_INCOMING—E.164 number or the username part of the SIP URI (the characters that precede the @ symbol in the SIP URI) of the calling endpoint (caller). • MEETME_OUTGOING—Internal number of the media bridge resource that initiated the dial out call.
Organization (also known as callerOrganization)	The value of the Organization field is dependent on the Call Type as follows: • DIRECTDIAL—Organization of the calling endpoint (caller). • MEETME_INCOMING—Organization of the calling endpoint (caller). • MEETME_OUTGOING—Organization of the meeting scheduler. **Note** If the Cisco TelePresence Exchange System cannot determine a value for this field, the value is null.

Table 12-4 CDR Field Descriptions for Fields Displayed on the CDRs Window (continued)

Field	Description
Callee	The value of the Callee field is dependent on the Call Type as follows: • DIRECTDIAL—E.164 number or the username part of the SIP URI (the characters that precede the @ symbol in the SIP URI) of the called endpoint (callee). • MEETME_INCOMING—Service number that the calling endpoint (caller) dials to reach the service for the meeting. • MEETME_OUTGOING—E.164 number or the username part of the SIP URI (the characters that precede the @ symbol in the SIP URI) of the called endpoint (callee).
Organization (also known as calleeOrganization)	The value of the Organization field is dependent on the Call Type as follows: • DIRECTDIAL—Organization of the called endpoint (callee). • MEETME_INCOMING—Organization of the meeting scheduler. • MEETME_OUTGOING—Organization of the called endpoint (callee). **Note** If the Cisco TelePresence Exchange System cannot determine a value for this field, the value is null.
Call Type	The Call Type field contains one of the following string values: • DIRECTDIAL—Direct Dial call. • MEETME_INCOMING—Call leg originates from an endpoint and connects to a Meet-Me or Rendezvous meeting on the Cisco TelePresence Exchange System. • MEETME_OUTGOING—Call leg for a Meet-Me or Rendezvous meeting originates from the Cisco TelePresence Exchange System and connects to an endpoint (for example, dial out calls to H.323, ISDN, or SIP endpoints). **Note** For call records imported from the Cisco Unified Communications Manager, the call type is DIRECTDIAL.
MeetMe Conf ID (Also known as meetingID)	Unique identifier for a Meet-Me or Rendezvous meeting. This is the number that the participant dials from the endpoint keypad to access the meeting after dialing the main access number. **Note** For direct dial calls or if the participant never joins the meeting, the value for this field is null.
Start Time	The time the called endpoint (callee) answers the call. The time is in ISO8601 format.
End Time	Time the Caller or Callee disconnects from the call. The time is in ISO8601 format.

Table 12-5 CDR Field Descriptions for Fields Displayed in Exported .csv File

Field	Description
icid (also known as guid)	Globally unique identifier for a call. The CDR for each call leg contains the same GUID.
legid	Unique identifier for a call leg.
startTime	The time the called endpoint (callee) answers the call. The time is in ISO8601 format.
endTime	Time the Caller or Callee disconnects from the call. The time is in ISO8601 format.
duration	Length of time in minutes from the startTime to the endTime of the call.
callType	The callType field contains one of the following string values: • DIRECTDIAL—Direct Dial call. • MEETME_INCOMING—Call leg originates from an endpoint and connects to a Meet-Me or Rendezvous meeting on the Cisco TelePresence Exchange System. • MEETME_OUTGOING—Call leg for a Meet-Me or Rendezvous meeting originates from the Cisco TelePresence Exchange System and connects to an endpoint (for example, dial out calls to H.323, ISDN, or SIP endpoints). **Note** For call records imported from the Cisco Unified Communications Manager, the call type is DIRECTDIAL.
cdrSource (also known as companyScope)	The companyScope field is relevant only for the DIRECTDIAL callType. This field contains one of the following string values: • CUCM_INTRACOMPANY—Intra-company direct dial calls that reside on Cisco Unified Communication Manager. • SERVICE_CONTROLLER—Inter-company direct dial calls.
serverName	Hostname of the call engine that the administrator assigns during installation.
serverIP	IP address of the call engine.
disconnectCauseCode	Q.850 or SIP cause code.
disconnectCauseStr	Text description of the disconnect cause.
disconnectData	Additional information to describe the disconnect cause.

Table 12-5 CDR Field Descriptions for Fields Displayed in Exported .csv File (continued)

Field	Description
address0 (also known as caller)	The value of the caller field is dependent on the callType as follows: • DIRECTDIAL—E.164 number or the username part of the SIP URI (the characters that precede the @ symbol in the SIP URI) of the calling endpoint (caller). • MEETME_INCOMING—E.164 number or the username part of the SIP URI (the characters that precede the @ symbol in the SIP URI) of the calling endpoint (caller). • MEETME_OUTGOING—Internal number of the media bridge resource that initiated the dial out call.
alternateIdentities0 (also known as callerAlternateIdentities)	Alternate identifier of the calling endpoint (caller), such as an IP address.
serviceProvider0 (also known as callerServiceProvider)	The value of the callerServiceProvider field is dependent on the callType as follows: • DIRECTDIAL—Service provider of the calling endpoint (caller). • MEETME_INCOMING—Service provider of the calling endpoint (caller). • MEETME_OUTGOING—Service provider hosting the meeting. **Note** If the Cisco TelePresence Exchange System cannot determine a value for this field, the value is null.
location0 (also known as callerRegion)	The value of the callerRegion field is dependent on the callType as follows: • DIRECTDIAL—Region of the service provider SBC of the calling endpoint (caller). • MEETME_INCOMING—Region of the service provider SBC of the calling endpoint (caller). • MEETME_OUTGOING—Region in which the media bridge resource allocated for the meeting is hosted. **Note** If the Cisco TelePresence Exchange System cannot determine a value for this field, the value is null.

Table 12-5 CDR Field Descriptions for Fields Displayed in Exported .csv File (continued)

Field	Description
organization0 (also know as callerOrganization)	The value of the callerOrganization field is dependent on the callType as follows: • DIRECTDIAL—Organization of the calling endpoint (caller). • MEETME_INCOMING—Organization of the calling endpoint (caller). • MEETME_OUTGOING—Organization of the meeting scheduler. **Note** If the Cisco TelePresence Exchange System cannot determine a value for this field, the value is null.
address1 (also known as callee)	The value of the callee field is dependent on the callType as follows: • DIRECTDIAL—E.164 number or the username part of the SIP URI (the characters that precede the @ symbol in the SIP URI) of the called endpoint (callee). • MEETME_INCOMING—Service number that the calling endpoint (caller) dials to reach the service for the meeting. • MEETME_OUTGOING—E.164 number or the username part of the SIP URI (the characters that precede the @ symbol in the SIP URI) of the called endpoint (callee).
alternateIdentities1 (also known as calleeAlternateIdentities)	Alternate identifier of the called endpoint (callee), such as an IP address.
serviceProvider1 (also known as calleeServiceProvider)	The value of the calleeServiceProvider field is dependent on the callType as follows: • DIRECTDIAL—Service provider of the called endpoint (callee). • MEETME_INCOMING—Service provider hosting the meeting. • MEETME_OUTGOING—Service provider of the called endpoint (callee). **Note** If the Cisco TelePresence Exchange System cannot determine a value for this field, the value is null.

Table 12-5 CDR Field Descriptions for Fields Displayed in Exported .csv File (continued)

Field	Description
location1 (also known as calleeRegion)	The value of the calleeRegion field is dependent on the callType as follows: • DIRECTDIAL—Region of the service provider SBC of the called endpoint (callee). • MEETME_INCOMING—Region in which the media bridge resource allocated for the meeting is hosted. • MEETME_OUTGOING—Region of the service provider SBC of the called endpoint (callee). **Note** If the Cisco TelePresence Exchange System cannot determine a value for this field, the value is null.
organization1 (also know as calleeOrganization)	The value of the calleeOrganization field is dependent on the callType as follows: • DIRECTDIAL—Organization of the called endpoint (callee). • MEETME_INCOMING—Organization of the meeting scheduler. • MEETME_OUTGOING—Organization of the called endpoint (callee). **Note** If the Cisco TelePresence Exchange System cannot determine a value for this field, the value is null.
meetingID	Unique identifier for a Meet-Me or Rendezvous meeting. This is the number that the participant dials from the endpoint keypad to access the meeting after dialing the main access number. **Note** For direct dial calls or if the participant never joins the meeting, the value for this field is null.
meetingJoinTime (also known as conferenceParticipantJoinTime	Time that the meeting participant joined the meeting. The time is in ISO8601 format. **Note** The Cisco TelePresence Exchange System does not consider the participant as having joined the meeting until after any interaction with the IVR prompts is complete.

Viewing Intra-Company CDRs

Intra-company (direct dial) calls are not routed via the Cisco TelePresence Exchange System cluster. As a result, the Cisco TelePresence Exchange System by default is not aware of these calls and does not generate any CDRs for them. Therefore, if you need to view intra-company CDRs, you must configure the Cisco TelePresence Exchange System to periodically import the CDRs from Cisco Unified Communications Manager.

Note

- The collected CDRs are stored on the Cisco TelePresence Exchange System with all the other CDRs.
- CDRs are imported hourly, and the timing for collection is also dependent on the schedule for CDR files being generated in Unified CM. Unless by chance a call comes in at exactly the right time to be included in the Unified CM processing and the Cisco TelePresence Exchange System processing immediately, you may need to wait an hour or two before the CDR appears in the database.

For detailed instructions, see the following "Configuring Unified CM to Enable Intra-Company CDRs" section on page 12-17.

Configuring Unified CM to Enable Intra-Company CDRs

To configure Cisco Unified Communications Manager to enable intra-company CDRs and then to provision the Unified CM publisher node in the Cisco TelePresence Exchange System administration console, do the following two procedures in the order presented.

Procedure

Step 1 Log in to the Cisco Unified Communications Manager publisher node as the administrator.

Step 2 From the Navigator menu, select **Cisco Unified Serviceability** and click **Go**.

Step 3 Choose **Tools > Service Activation**.

Step 4 From the Select Server drop-down list, select the publisher node.

Step 5 Verify that under the CDR Services menu, both the **Cisco SOAP – CDRonDemand Service** and the **Cisco CAR Web Service** check boxes are checked. If they are not checked, check them and click **Save** to activate these services.

Step 6 To create a custom API user for the CDR APIs in Unified CM, from the navigation menu, select **Unified CM Administration** and click **Go**.

Note The default ccmadministrator user can be used instead of the custom API user. However, for security reasons, Cisco recommends that a separate API user be created for the Cisco TelePresence Exchange System application to pull the CDRs from Unified CM.

Step 7 Choose **User Management > Application User** and click **New** to create a new application user.

Step 8 Choose **User Management > User Group** and click **Standard CAR Admin Users**.

Step 9 Click **Add App Users to Group** and select the application user that you created in Step 7.

Step 10 Repeat Step 8 and Step 9 for **Standard CCM End Users** and **Standard CCM Read Only**.

Step 11 To configure required enterprise parameters for a successful CDR import, do the following substeps:

a. Choose **System > Enterprise Parameters**.

b. In the **Allowed CDRonDemand get_file Queries Per Minute** field, enter 20.

c. In the **Allowed CDRonDemand get_file_list Queries Per Minute** field, enter 40.

d. Click **Save**.

Step 12 After changing the enterprise parameters, you must restart the Cisco Tomcat service on each of the servers in the cluster. Do the following substeps to restart the service.

a. From the Navigator menu, select **Cisco Unified Serviceability** and click **Go**.

b. Choose **Tools > Control Center - Network Services**.

c. At the top of the page, choose a server on which to restart Cisco Tomcat.

d. Under **Platform Services**, choose **Cisco Tomcat**.

e. At the bottom of the page, click **Restart**.

f. Repeat substeps c. through e. for each remaining server in the cluster.

Step 13 Continue with the following procedure to provision Unified CM in the Cisco TelePresence Exchange System administration console.

Procedure

Step 1 In the Cisco TelePresence Exchange System administration console, from the navigation pane, choose **Media Resources > Unified CM Resources**.

Step 2 Enter or edit information on the applicable Unified CM page to indicate the address of the Unified CM and the username and password of the API user that you created in Step 7 of the previous procedure.

Step 3 Click **Test Connection** to validate the username and password that you entered in Step 2.

When both Unified CM and the Cisco TelePresence Exchange System have been configured correctly to enable intra-company CDRs, the message “Connection has been verified.” is displayed.

When there is a mismatch in the credentials, the error message “Connection failed verification. Error accessing API.” is displayed. Verify the login credentials and if necessary the Host address of the Unified CM and repeat Step 3 until the “Connection has been verified” message is displayed.

CHAPTER 13

Configuring Collaboration Services

Revised July 3, 2012

The following sections describe how to configure collaboration services:

Configuring Service Numbers

The service number is the string of digits that users dial to reach the associated service. You can create custom service numbers (with associated custom IVR prompts) for each service provider.

The following sections describe how to configure service numbers:

Adding Service Numbers

Before You Begin

Configure the service provider and IVR prompt set that are associated with the service number.

Procedure

To add a new service number, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Service Numbers**.

The Service Numbers window is displayed.

Step 2 From the toolbar, click **Add A New Service Number**.

Step 3 Enter the settings as appropriate.

Table 13-1 describes the fields.

Step 4 To save your changes, click **Save**.

Editing Service Numbers

Procedure

To edit a service number, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Service Numbers**.

The Service Numbers window is displayed.

Step 2 In the item table, click the applicable entry.

Step 3 From the toolbar, click **Edit This Service Number**.

The details for the service number is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as appropriate.

Table 13-1 describes the fields.

Step 5 To save your changes, click **Save**.

Deleting Service Numbers

Procedure

To delete a service number, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Service Numbers**.

The Service Numbers window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple service numbers at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a service number prior to deleting it, in the Service Numbers window, you can click the applicable **Service Number** to go to the Service Number page. After verifying that you have chosen the correct service number to delete, click **Delete This Service Number**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Service Number Fields

Table 13-1 Service Number Field Descriptions

Field	Description
Number	The string of digits that users dial to reach this service. You can enter up to 32 characters (which can include dashes, underscores, and parentheses after the first character).
Name	Text string used to identify this service number when scheduling a meeting.
Description	Text string describing this service number. See the "Common Field Properties" section on page 2-4.
Service	Drop-down list of the available services. Choose the service that you want to associate with this service number.
Service Provider	Drop-down list of the available service providers. Choose the service provider that you want to associate with this service number. See the "Adding Service Providers" section on page 10-1.
IVR Prompt	Drop-down list of the available sets of IVR prompts. For example, you can define a set of IVR prompts such as a welcome message and a help desk message for an organization. Choose the IVR prompt set that you want to associate with this service number. See the "Adding IVR Prompts" section on page 13-5.

Configuring IVR Prompts

Cisco routers store voice files that provide interactive voice response (IVR) prompts to users in response to certain activities. For example, you can define IVR prompts to welcome users to a call, to request a meeting ID when a user calls in, to indicate that the meeting has not yet started, or to direct users to the help desk.

Service Providers can configure custom IVR prompts for each organization or for different languages. When scheduling a meeting, you specify a the name of a service number, which dictates which prompt set is used for the meeting.

Note In order to play IVR prompts in the administration console, the browser requires a media player plug-in capable of playing the .au audio file format.

The following sections describe how to configure IVR prompts:

Default Cisco IVR Prompts for Lab Use

The Cisco TelePresence Exchange System comes preloaded with a default Cisco IVR prompt set called CTX Default Ivr Prompts. You can rename, replace or delete the default Cisco IVR prompt set. However, the system will replace the prompt set in its original form the next time the call engine servers restart. For this reason, we recommend that you do not rename the default set or create a different set with the same name.

Note The default Cisco prompts are provided for lab use only. In production, you must use one or more custom prompt sets rather than the default Cisco prompts.

Table 13-2 describes the default IVR prompts.

Table 13-2 Default Cisco IVR Prompt Messages

Prompt	Prompt Message
Welcome Prompt	Welcome to the Cisco TelePresence Conferencing Service.
Invalid Meeting Prompt	The conference ID that you entered is invalid.
Helpdesk Prompt	Please wait while we connect you to a Help Desk representative.
Max Participants Prompt	Your call cannot be connected to the meeting you requested because the meeting's maximum number of participants have been reached.
Meeting Not Started Prompt	The meeting that you requested has not yet started. Check the meeting schedule and call back at the scheduled start time.
Request ID Prompt	Please enter your conference ID.
Timeout Prompt	I did not receive your input.
Unauthorized Prompt	Your call cannot be connected because the number you dialed from is not authorized to use the Cisco TelePresence Conferencing Service. To obtain assistance or for additional information about this service, call Cisco TelePresence Conferencing Service Help Desk.
Valid Meeting Prompt	Please wait while we connect you to your meeting.
GoodBye Prompt	Thank you for using the Cisco TelePresence Conferencing Service. Goodbye.
No Conference Resource Available Prompt	All conferencing resources are busy at this time. Please try your call again later.
Meeting Locked Prompt	The conference ID that you entered is currently locked. Please contact your help desk for assistance.
Enter Host PIN Prompt	If you are the meeting host, enter your PIN now. Otherwise, please wait for the host to start the meeting.
Host Join Timeout Prompt	The meeting host has not joined the meeting within the allotted time. Please contact the Help Desk for assistance with this meeting.
Incorrect Host PIN Prompt	The host PIN entered is not valid. Please try again.

Table 13-2 Default Cisco IVR Prompt Messages

Prompt	Prompt Message
Transfer From Waiting Room Prompt	You will now be transferred to the meeting.
Host PIN Helpdesk Transfer Prompt	The host PIN entered is not valid.

Adding IVR Prompts

Before You Begin

Install and configure the Cisco router.

Record or locate a prompt or prompt set that is recorded in 8-bit mu-Law encoded NeXT/Sun AU audio format, 8000Hz, 16-bit Mono.

Procedure

To add a new IVR prompt or set of IVR prompts, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > IVR Prompts**.

The IVR Prompts window is displayed.

Step 2 From the tool bar, click **Add A New IVR Prompt**.

Step 3 Enter the settings as appropriate.

Table 13-3 describes the fields.

Step 4 To save your changes, click **Save**.

Related Topics

To configure prompts on the Cisco router, see the "Configuring the Cisco Router with IVR" chapter.

Editing IVR Prompts

Procedure

To edit the IVR prompts, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > IVR Prompts**.

The IVR Prompts window is displayed.

Step 2 In the item table, click the applicable entry.

The IVR Prompt Overview window for the IVR prompt is displayed.

Step 3 From the toolbar, click **Edit This IVR Prompt**.

The Edit IVR Prompts window is displayed. You can click **Play** to hear the existing recording for each prompt.

Step 4 To replace an existing IVR file, click **Upload** for the entry and browse for the replacement file.

Table 13-3 describes each field.

Step 5 To save your changes, click **Save**.

Deleting IVR Prompts

Procedure

To delete IVR prompts, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > IVR Prompts**.

The IVR Prompts window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple IVR prompts at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of an IVR prompt prior to deleting it, in the IVR Prompts window, you can click the applicable **IVR Prompt** to go to the IVR Prompt page. After verifying that you have chosen the correct IVR prompt to delete, click **Delete This IVR Prompt**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

IVR Prompt Fields

Table 13-3 IVR Prompt Field Descriptions

Field	Description
Name	Text string identifying the group of IVR prompts. See the "Common Field Properties" section on page 2-4. **Note** Do not use a name that matches the name of the default Cisco IVR prompt set.
Description	Text string describing the group of IVR prompts. See the "Common Field Properties" section on page 2-4.
Welcome Prompt	Text string indicating the location of the voice file for the Welcome prompt.
Invalid Meeting Prompt	Text string indicating the location of the voice file for the Invalid Meeting prompt.

Table 13-3 IVR Prompt Field Descriptions (continued)

Field	Description
Helpdesk Prompt	Text string indicating the location of the voice file for the Helpdesk prompt.
Max Participants Prompt	Text string indicating the location of the voice file for the Maximum Participants prompt.
Meeting Not Started Prompt	Text string indicating the location of the voice file for the Meeting Not Started prompt.
Request ID Prompt	Text string indicating the location of the voice file for the Request Id prompt.
Timeout Prompt	Text string indicating the location of the voice file for the Timeout prompt.
Unauthorized Prompt	Text string indicating the location of the voice file for the Unauthorized prompt.
Valid Meeting Prompt	Text string indicating the location of the voice file for the Valid Meeting prompt.
GoodBye Prompt	Text string indicating the location of the voice file for the GoodBye prompt.
No Conference Resource Available Prompt	Text string indicating the location of the voice file for the No Conference Resource Available prompt.
Meeting Locked Prompt	Text string indicating the location of the voice file for the Meeting Locked prompt.
Enter Host PIN Prompt	Text string indicating the location of the voice file for the Enter Host PIN prompt.
Host Join Timeout Prompt	Text string indicating the location of the voice file for the Host Join Timeout prompt.
Incorrect Host PIN Prompt	Text string indicating the location of the voice file for the Incorrect Host PIN prompt.
Transfer From Waiting Room Prompt	Text string indicating the location of the voice file for the Transfer From Waiting Room prompt.
Host PIN Helpdesk Transfer Prompt	Text string indicating the location of the voice file for the Host PIN Helpdesk Transfer prompt.

Scheduling Meetings

You can view the scheduled meetings on this Cisco TelePresence Exchange System, and you can schedule meetings.

The following sections describe how to schedule meetings and how to view existing meetings:

- Viewing Meetings, page 13-8
- Scheduling Meetings, page 13-8
- Canceling Meetings, page 13-9
- Deleting Meetings, page 13-9

- Schedule Meeting Fields for Meet-Me Meetings, page 13-11
- Schedule Meeting Fields for Remote Meetings, page 13-17
- Schedule Meeting Fields for Two-Party Direct Meetings, page 13-19
- Meeting Details Fields for Meet-Me, Remote, and Two-Party Direct Meetings, page 13-20

For information on meeting diagnostics, see the "Meeting Diagnostics" chapter.

Note For information on scheduling Rendezvous meetings, see the "Scheduling Rendezvous Meetings" section on page 13-22.

Viewing Meetings

Procedure

To view the meetings scheduled on this Cisco TelePresence Exchange System, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

By default, this window displays all meetings from12:00 am (0000) of the current day, in your time zone, and one week from the current day. Meetings are sorted in ascending order by start time.

Tip To view all meeting information on the system, click **Clear Filters**.

For information on how to use the sorting and filtering options, see the "Sorting and Filtering Lists in the Administration Console" section on page 2-5.

Note The system uses the default filter options each time you choose a menu option.

Step 2 To view information about a meeting in the item table, click the subject of the applicable meeting to view the meeting details page. Table 13-7 lists the fields.

For information on how to view the meeting diagnostics for a meeting, see the "Meeting Diagnostics" chapter.

Scheduling Meetings

Procedure

To schedule a new meeting, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 2 To schedule a meeting, click **Add A New Meeting**.

Step 3 Enter the settings for the meeting.

The following tables describe the meeting fields, depending on the type of meeting you select:

- MeetMe—Table 13-4.
- Rendezvous—Table 13-8. (For more information about Rendezvous meetings, see the "Scheduling Rendezvous Meetings" section on page 13-22.)
- Remote—Table 13-5.
- Two Party Direct—Table 13-6.

Step 4 To save your changes, click **Schedule**.

Canceling Meetings

Users with the SERVICEDESK, ADMIN or SYSTEM role can cancel a meeting as long as there are no participants currently attending the meeting.

When you cancel a meeting, the Cisco TelePresence Exchange System frees up any ports of organization bandwidth or segments of guaranteed media bridge capacity associated with the meeting, and participants can no longer join the meeting.

After you cancel the meeting, the system continues to maintain the meeting details and diagnostics. To remove the details and diagnostics, see the "Deleting Meetings" section on page 13-9.

Procedure

To cancel a meeting, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 2 Click the applicable meeting to view the meeting details page.

Step 3 From the toolbar, click **Cancel This Meeting**.

Note You cannot cancel a meeting that is currently active.

Step 4 In the Cancellation Confirmation dialog box, check the **Cancel OBTP** check box.

Step 5 Click **OK** to confirm the cancellation.

Deleting Meetings

Users with the ADMIN or SYSTEM role can delete a meeting as long as there are no participants currently attending the meeting.

When you delete a meeting, the Cisco TelePresence Exchange System cancels the meeting if it has not been previously cancelled, frees up any ports of organization bandwidth or segments of guaranteed media bridge capacity associated with the meeting, and removes the meeting details and diagnostics.

To cancel the meeting without removing the details from the system, see the "Canceling Meetings" section on page 13-9.

Procedure

To delete a meeting, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 2 Click the applicable meeting to view the meeting details page.

Step 3 From the toolbar, click **Delete This Meeting**.

Note You cannot delete a meeting that is currently active.

Step 4 To confirm the cancellation and deletion, click **OK**.

Schedule Meeting Fields for Meet-Me Meetings

Table 13-4 Schedule Meeting Field Descriptions for Meet-Me Meetings

Field	Description
Basic Meeting Information	
Meeting Type	Radio buttons provide a choice of MeetMe, Rendezvous, Remote, or Two Party Direct. • MeetMe meeting—System reserves media resources for the meeting. The meeting can include provisioned endpoints, unprovisioned endpoints, and remote endpoints. By default, One-Button-to-Push (OBTP) information is displayed at locally provisioned endpoints unless you uncheck the **Push OBTP** check box. • Rendezvous—A meeting that does not have a preconfigured start time. Participants can join the meeting at any time. When one or more participants join a Rendezvous meeting, an instance of the meeting is created and the meeting is considered active. • Remote meeting—System does not reserve media resources for the meeting (the remote Cisco TelePresence Exchange System provides the media resources). OBTP information is displayed at locally provisioned endpoints. A remote meeting involves an inter-service provider participant. • Two Party Direct—System does not reserve media resources, because this type of meeting is direct-dialed. However, you can specify the service provider, scheduler, and meeting details (start time and duration). **Note** You can set up a two party direct meeting for two separate organizations, as long as both organizations are on the same Cisco TelePresence Manager.
Subject	Text description of the meeting.
Start Time	Date, start time, and time zone of the meeting. Text field or calendar to specify the date. Text field to specify the hour. Drop-down list to choose AM or PM. Drop-down list to choose the time zone. **Note** The Cisco TelePresence Exchange System reserves resources based on fifteen-minute increments on the hour (for example, 9:00, 9:15, 9:30, or 9:45). Choose a start time consistent with these time periods. For example, choose a start time of 9:30 am or 9:45 am rather than 9:40 am.
Duration	Duration of the meeting in minutes. **Note** The Cisco TelePresence Exchange System reserves resources based on fifteen-minute increments on the hour (for example, 9:00, 9:15, 9:30, or 9:45). Choose a duration consistent with these increments. For example, choose a duration of 30 or 45 minutes rather than 35 minutes.

Table 13-4 Schedule Meeting Field Descriptions for Meet-Me Meetings (continued)

Field	Description
Service Provider	Drop-down list of service providers. Choose the service provider that will host this meeting.
Scheduler	Email address of the contact person for the meeting. When you enter this information, it is displayed on the telepresence IP phone during the meeting. This is useful if there is an issue with the meeting.
Scheduler's Organization	Drop-down list of the available organizations. Choose the organization of the scheduler to apply to the meeting. This field is required to enable service provider and organization inheritance capabilities. Some settings, such as automatic meeting extension and host settings, can be inherited. You can configure Meet-Me and Rendezvous meetings to inherit the settings from the meeting scheduler organization. Likewise, you can configure the organization to inherit the settings from the service provider. Service provider-level settings will be overridden if the inheritance option is not enabled at the organization level, and organization-level settings will be overridden if the inheritance option is not enabled at the meeting level. The scheduler organization is also used to determine the whitelist policy to apply to intra- and inter-service provider calls.
Reservation Type	Drop-down list of reservation types. Choose the reservation type to apply to the meeting. The reservation type determines whether the system provides guaranteed or best-effort service when reserving media bridge resources for the meeting, and the system selects a resource group based on the reservation type and other meeting parameters.
Geographic Settings	
Region	Drop-down list of regions. Choose the region where the meeting will be hosted. The system reserves media resources at a media POP in this region.
Service Number Name	Drop-down list of service number names. Choose the name of the service number that users dial to reach the service for the meeting. **Note** The service number that you choose also determines which set of IVR prompts play to attendees in response to certain conditions, such as joining or leaving the meeting, being prompted for the conference ID or host PIN, or encountering problems.

Table 13-4 Schedule Meeting Field Descriptions for Meet-Me Meetings (continued)

Field	Description
Endpoint Provisioning Options	
Provisioned Endpoints	Endpoints for which all configuration details (such as name, phone number, number of screens, and organization) are known by the administrator and configured on the system. Click **Add Provisioned Endpoints** to add an endpoint and configure the following values: • **Endpoint Organization**—Drop-down list of organizations that are associated with the Service Provider configured for the meeting. • **Endpoint Name**—Drop-down list of endpoints associated with the Endpoint Organization. • **Ports—**Number of segments of organization bandwidth that the endpoint requires. The default value is zero. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.) • **Dial Out—**Check this check box to have the system dial out to reach the endpoint. • **Host**—Check this check box to designate this endpoint as a host. Applicable only when the host and guest roles are enabled. To add an additional endpoint, click **Add Provisioned Endpoints** again.
Unprovisioned Endpoints	Endpoint for which no configuration details are known by the administrator except the name of the meeting scheduler for that endpoint. Click **Add Unprovisioned Endpoints** to add an unprovisioned endpoint and configure the following values: • **Bandwidth-Providing Organization**—Drop-down list of organizations that are associated with the Service Provider configured for the meeting. • **Ports—**Number of segments of organization bandwidth that the endpoint requires. The default value is zero. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.) • **Guest Dial Out**—Check this check box to have the system dial out to reach the endpoint. • **Number**—Number that the system must dial to reach the endpoint. • **Media Profile**— (Optional) If the system is dialing out to the endpoint, you can specify the media profile in order to tailor the bridge selection and capacity calculation to your needs. The default assumption is a single-screen H.323 media profile. To add an additional endpoint, click **Add Unprovisioned Endpoints** again.

Table 13-4 Schedule Meeting Field Descriptions for Meet-Me Meetings (continued)

Field	Description
Remote Endpoints	Reserves capacity for a remote endpoint for an inter-service provider participant. No additional data is visible or configurable for this type of endpoint. To reserve capacity for a remote endpoint, click **Add Remote Endpoints**. A Remote Endpoint entry is displayed on the window. No additional configuration is possible.
Additional Media Profiles	Allows you to specify additional media profiles so that the Cisco TelePresence Exchange System can choose the correct bridge resource type on which to reserve the meeting based on the capacity and capabilities required by unexpected or unspecified endpoints that may join the meeting. For example, if only CTS endpoints are added to a meeting, the system will try to reserve CTMS resources for the meeting. If you add the built-in Default Generic H.323 media profile, then the system will try to reserve a TPS resource or MSE 8510. To choose a media profile to include in the meeting, click **Add Media Profiles**.
Meeting Extension Options	
Meeting Extension	Radio buttons provide a choice of Disabled, Enabled, or Inherit from Organization. • Disabled—The system does not automatically extend the meeting, regardless of resource availability. • Enabled—The system automatically extends the meeting if resources are available near the end of the meeting. The system checks for available resources shortly before the two minute end-of-meeting warning. If sufficient resources are available, the meeting continues for the length of time specified in the Meeting Extension Period field, and may extend again near the end of that period if the number of extensions specified by Max Meeting Extensions Allowed has not been exceeded. If the extension fails, the system displays the two minute end-of-meeting warning to participants, and ends the meeting after two minutes. • Inherit from Organization—Use the Meeting Extension settings configured for the Scheduler's Organization. The organization may be configured to inherit these settings from the service provider to which the organization belongs. **Note** You can configure the meeting extension policy at the service provider level, organization level, or meeting level. The policy is hierarchical, so you can configure a meeting to inherit its settings from the meeting scheduler organization. In addition, you can configure an organization to inherit its settings from the service provider. If you want a meeting to inherit organization settings, you must enable the inheritance option at the meeting level. Similarly, if you want an organization to inherit service provider settings, you must enable the inheritance option at the organization level.

Table 13-4 Schedule Meeting Field Descriptions for Meet-Me Meetings (continued)

Field	Description
Meeting Extension Period (minutes)	*Available only if Meeting Extension is set to Enabled.* Specify the length by which to automatically extend the meeting if resources are available when the meeting nears its configured duration. The extension length must be a multiple of 15 (for example, 15, 30 or 45).
Max Meeting Extensions Allowed	*Available only if Meeting Extension is set to Enabled.* Specify the maximum number of times the meeting can be extended if resources are available. The maximum number of extensions times the Meeting Extension Period must not exceed 1440 minutes (24 hours). **Note** If an administrator or service desk user extends the meeting duration while the meeting is active, the extension counter is reset, and the next extension after the change is counted as the first extension.
Host/Guest Options	
Enable Host/Guest Roles	Check box. Check this check box to enable host and guest options for the meeting.
Drop Participants On Host Exit	*Applicable only when Enable Host/Guest Roles is checked.* Radio buttons provide a choice of the following conditions. • False—The system does not drop any participants when the host leaves the meeting. • True—The system drops all participants from the meeting when the host leaves. If the meeting has more than one host, participants will be dropped when all hosts have left the meeting. • Inherit from Organization—Use the host and guest settings configured for the organization. **Note** You can configure the host settings at the service provider level, organization level, or meeting level. The policy is hierarchical, so you can configure a Meet-Me or Rendezvous meeting to inherit its settings from the meeting scheduler organization. In addition, you can configure an organization to inherit its settings from the service provider. If you want a meeting to inherit organization settings, you must enable the inheritance option at the meeting level. Similarly, if you want an organization to inherit service provider settings, you must enable the inheritance option at the organization level.
Host PIN	*Applicable only when Enable Host/Guest Roles is checked.* Radio buttons provides the following choices: • Auto-Generate—The system creates a host PIN that a participant must enter to join the meeting as a host. • Customize—The meeting scheduler specifies a custom host PIN that a participant must enter to join the meeting as a host.

Table 13-4 Schedule Meeting Field Descriptions for Meet-Me Meetings (continued)

Field	Description
Custom Host PIN	*Applicable only when Enable Host/Guest Roles is checked, and Customize is selected for the Host PIN.* The PIN that a participant must enter to join the meeting as a host. The PIN must be 6 digits long.
Advanced Options	
Additional Capacity	Number of additional segments of media bridge capacity that the system needs to reserve for the meeting. Use this field to allocate media bridge resources for endpoints that are not configured to be part of the meeting but that you expect to join the meeting. To determine how many segments to add for each endpoint, use the following guidelines, depending on which media resource provides the meeting bridge: • Cisco TelePresence Multipoint Switch—Add 4 segments for each three-screen endpoint and 2 segments for each single-screen endpoint. • Cisco TelePresence Server MSE 8710—Add 3 segments for each three-screen endpoint and 1 segment for each single-screen endpoint. • Cisco TelePresence MCU MSE 8510—Add 1 segment. The MCU MSE 8510 supports only single-screen endpoints. **Note** The Additional Capacity field does not affect the amount of organization bandwidth that is reserved for the meeting. Organization bandwidth is determined by the value of the **Ports** field that is configured for each provisioned and unprovisioned endpoint that is added to the meeting. For more information on capacity reservation and bridge selection, see Appendix B, "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection."
Conference ID	Text field. Enter a unique, eight-digit conference ID for users to dial to reach this meeting. **Note** The Conference ID is optional. If you do not enter an ID, the system will generate one for you.
Push OBTP	Check box. Check the check box if you want the system to send One-Button-to-Push (OBTP) information to the IP phones in the rooms that are associated with the provisioned endpoints.
Custom Screen Layout (Used on MSE 8510)	For meetings on MSE 8510, select the screen layout used to display participant video.

Schedule Meeting Fields for Remote Meetings

Table 13-5 Schedule Meeting Field Descriptions for Remote Meetings

Field	Description
Basic Meeting Information	
Meeting Type	Radio buttons provide a choice of MeetMe, Rendezvous, Remote, or Two Party Direct. • MeetMe meeting—System reserves media resources for the meeting. The meeting can include provisioned endpoints, unprovisioned endpoints, and remote endpoints. By default, One-Button-to-Push (OBTP) information is displayed at locally provisioned endpoints unless you uncheck the **Push OBTP** check box. • Rendezvous—A meeting that does not have a preconfigured start time. Participants can join the meeting at any time. When one or more participants join a Rendezvous meeting, an instance of the meeting is created and the meeting is considered active. • Remote meeting—System does not reserve media resources for the meeting (the remote Cisco TelePresence Exchange System provides the media resources). OBTP information is displayed at locally provisioned endpoints. A remote meeting involves an inter-service provider participant. • Two Party Direct—System does not reserve media resources, because this type of meeting is direct-dialed. However, you can specify the service provider, scheduler, and meeting details (start time and duration). **Note** You can set up a two party direct meeting for two separate organizations, as long as both organizations are on the same Cisco TelePresence Manager.
Subject	Text description of the meeting.
Start Time	Date, start time, and time zone of the meeting. Text field or calendar to specify the date. Text field to specify the hour. Drop-down list to choose AM or PM. Drop-down list to choose the time zone. **Note** The Cisco TelePresence Exchange System reserves resources based on fifteen-minute increments on the hour (for example, 9:00, 9:15, 9:30, or 9:45). Choose a start time consistent with these time periods. For example, choose a start time of 9:30 am or 9:45 am rather than 9:40 am.
Duration	Duration of the meeting in minutes.
Service Provider	Drop-down list of service providers. Choose the service provider that will host this meeting.
Scheduler	Email address of the contact person for the meeting. When you enter this information, it is displayed on the telepresence IP phone during the meeting. This is useful if there is an issue with the meeting.

Table 13-5 Schedule Meeting Field Descriptions for Remote Meetings (continued)

Field	Description
Connection Information	
Conference ID	Text field. Enter the conference ID configured for the meeting on the remote system.
Access Number	Number that the participant must call to reach the meeting.
Endpoint Provisioning Options	
Provisioned Endpoints	Click **Add Provisioned Endpoints** to add an endpoint and configure the following values: • **Endpoint Organization**—Drop-down list of organizations that are associated with the Service Provider configured for the meeting. • **Endpoint Name**—Drop-down list of endpoints associated with the Endpoint Organization. • **Ports—**Number of segments of organization bandwidth that the endpoint requires. The default value is zero. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.) To add an additional endpoint, click **Add Provisioned Endpoints** again.
Unprovisioned Endpoints	Unprovisioned meetings reserve ports or organization bandwidth for an unknown endpoint for a specific organization. Click **Add Unprovisioned Endpoints** and configure the following values: • **Bandwidth-Providing Organization**—Drop-down list of organization names, and choose an organization to include in this meeting. • **Ports**—Number of segments of organization bandwidth that the endpoint requires. The default value is zero. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.) To add an additional endpoint, click **Add Unprovisioned Endpoints** again.

Schedule Meeting Fields for Two-Party Direct Meetings

Table 13-6 Schedule Meeting Field Descriptions for Two-Party Direct Meetings

Field	Description
Basic Meeting Information	
Meeting Type	Radio buttons provide a choice of MeetMe, Rendezvous, Remote, or Two Party Direct. • MeetMe meeting—System reserves media resources for the meeting. The meeting can include provisioned endpoints, unprovisioned endpoints, and remote endpoints. By default, One-Button-to-Push (OBTP) information is displayed at locally provisioned endpoints unless you uncheck the **Push OBTP** check box. • Rendezvous—A meeting that does not have a preconfigured start time. Participants can join the meeting at any time. When one or more participants join a Rendezvous meeting, an instance of the meeting is created and the meeting is considered active. • Remote meeting—System does not reserve media resources for the meeting (the remote Cisco TelePresence Exchange System provides the media resources). OBTP information is displayed at locally provisioned endpoints. A remote meeting involves an inter-service provider participant. • Two Party Direct—System does not reserve media resources, because this type of meeting is direct-dialed. However, you can specify the service provider, scheduler, and meeting details (start time and duration). **Note** You can set up a two party direct meeting for two separate organizations, as long as both organizations are on the same Cisco TelePresence Manager.
Subject	Text description of the meeting.
Start Time	Date, start time, and time zone of the meeting. Text field or calendar to specify the date. Text field to specify the hour. Drop-down list to choose AM or PM. Drop-down list to choose the time zone. **Note** The Cisco TelePresence Exchange System reserves resources based on fifteen-minute increments on the hour (for example, 9:00, 9:15, 9:30, or 9:45). Choose a start time consistent with these time periods. For example, choose a start time of 9:30 am or 9:45 am rather than 9:40 am.
Duration	Duration of the meeting in minutes.
Service Provider	Drop-down list of service providers. Choose the service provider that will host this meeting.
Scheduler	Email address of the contact person for the meeting. When you enter this information, it is displayed on the telepresence IP phone during the meeting. This is useful if there is an issue with the meeting.

Table 13-6 Schedule Meeting Field Descriptions for Two-Party Direct Meetings (continued)

Field	Description
Endpoint Provisioning Options	
Provisioned Endpoints	Click **Add Provisioned Endpoints** to add an endpoint and configure the following values: • **Endpoint Organization**—Drop-down list of organizations that are associated with the Service Provider configured for the meeting. • **Endpoint Name**—Drop-down list of provisioned endpoints associated with the Endpoint Organization. The list includes only endpoints that support One-Button-to-Push (OBTP), because the purpose of scheduling a two-party direct meeting is to provide OBTP for the endpoints. **Note** The two endpoints must be associated with the same Cisco TelePresence Manager resource. To add an additional endpoint, click **Add Provisioned Endpoints** again.

Meeting Details Fields for Meet-Me, Remote, and Two-Party Direct Meetings

Table 13-7 Meeting Details Field Descriptions

Field	Description
Overview Tab	
Subject	Text description of the meeting.
Start Time	Date, start time, and time zone of the meeting.
Duration	Scheduled duration of the meeting in minutes.
Scheduler	Email address of the contact person for the meeting.
Service Provider	The service provider hosting the meeting.
Meeting Key	Unique identifier for the meeting. You can use the meeting key to identify this meeting in API requests.
Requested OBTP	Indicates whether the meeting was configured to send One-Button-to-Push (OBTP) information to the IP phones in the rooms that are associated with the provisioned endpoints.
Meeting Extension	Indicates whether the meeting was configured to be automatically extended if resources are available when the meeting nears the configured duration.
Meeting Extension Period	The length, in minutes, by which to automatically extend the meeting if Meeting Extension is enabled and resources are available when the meeting nears its configured duration.
Max Meeting Extensions	The maximum number of times the meeting can be extended if Meeting Extension is enabled and resources are available when the meeting nears its configured duration.
Meeting Type	Indicates the type of meeting: MeetMe, Rendezvous, remote, or two-party direct.

Table 13-7 Meeting Details Field Descriptions (continued)

Field	Description
Cancelled	Indicates whether the meeting was cancelled. When you cancel a meeting, the system frees up any ports of organization bandwidth or segments of guaranteed media bridge capacity associated with the meeting, and participants can no longer join the meeting. After you cancel the meeting, the system continues to maintain the meeting details and diagnostics unless you delete the meeting.
Meet-Me Info Tab (Displayed only for Meet-Me meetings that have not been cancelled)	
Scheduler's Organization	Organization to which the meeting scheduler belongs. The scheduler organization is used to determine the whitelist policy to apply to intra- and inter-service provider calls. It is also used when the automatic meeting extension or host features are configured to inherit their settings from the organization.
Remote Access Number	Number that users dial to reach the system if they dial in to the meeting rather than attending by using One-Button-to-Push (OBTP).
Conference ID	Unique, eight-digit ID that users are prompted to enter if they dial in to the meeting rather than attending by using One-Button-to-Push (OBTP).
Reserved Screens	Total number of segments of capacity that the system has reserved on the media bridge for the meeting. The total is based on the provisioned and unprovisioned endpoints that are added to the meeting plus the value entered in the Additional Capacity field.
Region	Region of the media bridge resource that is hosting the meeting.
Large Meeting	Indicates whether the system classifies the meeting as a Large Meeting. Large meetings include 32 or more segments and are scheduled exclusively on media units that are reserved for large meetings.
Bridge Resource Type	Type of bridge that is hosting the meeting: CTMS (Cisco TelePresence Multipoint Switch), TPS (Cisco TelePresence Server MSE 8710), or TPS_8510 (Cisco TelePresence MCU MSE 8510).
Reservation Type	Reservation type specified for the meeting. The reservation type determines whether the meeting is guaranteed (the system reserved media bridge resources for the meeting when it was scheduled) or not guaranteed (the system did not reserve media bridge resources at scheduling time).
Host/Guest Roles Enabled	Indicates whether host and guest options are enabled.
Remote Info Tab (Displayed only for remote meetings that have not been cancelled)	
Remote Access Number	Number that users dial to reach the system if they dial in to the meeting rather than attending by using One-Button-to-Push (OBTP).
Conference ID	Unique, eight-digit ID that users are prompted to enter if they dial in to the meeting rather than attending by using One-Button-to-Push (OBTP).
Provisioned Endpoints Tab (Displayed only for meetings that have provisioned endpoints configured)	
Endpoint	Cisco TelePresence Exchange System–provisioned name of the endpoint.

Table 13-7 Meeting Details Field Descriptions (continued)

Field	Description
Ports	Number of segments of organization bandwidth that the endpoint requires. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.)
Minimize Capacity	Indicates whether the Minimize Capacity check box is checked on the organization to which the endpoint belongs.
Dialout	Indicates whether the system is configured to dial out to reach the endpoint.
Is Host	Indicates whether the endpoint is designated as a meeting host.
Organization	Organization to which the endpoint is associated.
Unprovisioned Endpoints Tab (Displayed only for meetings that have unprovisioned endpoints configured)	
Ports	Number of segments of organization bandwidth that the endpoint requires. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.)
Organization	Organization to which the endpoint is associated.
Guest Dial Out	Indicates whether the system is configured to dial out to reach the endpoint.
Number	Phone number to dial to reach the endpoint (used if Guest Dial Out is true for the endpoint).
Media Profile	Media profile of the endpoint. At schedule time, the media profile helps tailor the bridge selection and capacity calculation to your needs. At attend time, the system determines the protocol to use when dialing out to the endpoint based on the protocols supported by the media profile and the type of bridge on which the meeting is hosted.
Remote Endpoints (Displayed only for meetings that have remote endpoints configured)	
Endpoint	Indicates that a remote endpoint has been configured for the meeting. The system displays “Remote Endpoint” for each remote endpoint that you add to the meeting.

Scheduling Rendezvous Meetings

You can add, modify, cancel, and delete Rendezvous meetings and view information about Rendezvous meetings that are added on the system.

Note Standing meetings are no longer supported on the Cisco TelePresence Exchange System as previously defined, but they have been replaced with an equivalent type of meeting. Instead of creating a standing meeting, create a Rendezvous meeting with a guaranteed reservation type.

For information on how to manage active meetings, see the “Managing Active Meetings” section on page 13-32.

The following sections describe how to maintain Rendezvous meetings:

Adding Rendezvous Meetings

Procedure

To add a new Rendezvous meeting to the system, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 2 From the toolbar, click **Schedule New Meeting**.

Step 3 Enter the settings for the meeting.

Table 13-8 describes the fields for scheduling Rendezvous meetings.

Step 4 To save your changes, click **Schedule**.

Viewing Rendezvous Meeting Information

Procedure

To view information about Rendezvous meetings that are added to the system, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed. The item table shows the meetings that have been created on the system.

By default, this window displays all meetings from12:00 am (0000) of the current day, in your time zone, and one week from the current day, sorted in ascending order by start time. Because Rendezvous meetings do not have a start time, these meetings are not displayed.

Tip To view all meeting information on the system, including Rendezvous meetings, click **Clear Filters**.

For information on how to use the sorting and filtering options, see the "Sorting and Filtering Lists in the Administration Console" section on page 2-5.

Note The system uses the default filter options each time you choose a menu option.

Step 2 To view information about a meeting in the item table, click the subject of the applicable meeting to view the meeting details page. Table 13-9 lists the fields.

For information on how to view the meeting diagnostics for a meeting, see the "Meeting Diagnostics" chapter.

Modifying Rendezvous Meetings

Note An active Rendezvous meeting can be modified only by using the Active Meeting Management feature.

Procedure

To modify a Rendezvous meeting, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 2 Click the applicable meeting to view the meeting details page.

Step 3 From the toolbar, click **Modify This Meeting**.

Fields displayed contain the currently-configured settings.

Note When you try to modify a meeting that is currently active, you get a modified version of the Modify This Meeting window, with some fields disabled. For more information, see the "Managing Active Meetings" section on page 13-32.

Step 4 Modify field entries as appropriate (see Table 13-8).

Step 5 To save your changes, click **Schedule**.

Canceling Rendezvous Meetings

Users with the SERVICEDESK, ADMIN or SYSTEM role can cancel a Rendezvous meeting as long as there are no participants currently attending the meeting.

When you cancel a Rendezvous meeting, the Cisco TelePresence Exchange System frees up any ports of organization bandwidth or segments of guaranteed media bridge capacity associated with the meeting, and participants can no longer join the meeting.

After you cancel the meeting, the system continues to maintain the meeting details and diagnostics. To remove the details and diagnostics, see the "Deleting Rendezvous Meetings" section on page 13-25.

Procedure

To cancel a Rendezvous meeting, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 2 Click the applicable meeting to view the meeting details page.

Step 3 From the toolbar, click **Cancel This Meeting**.

Note You cannot cancel a meeting that is currently active.

Step 4 In the Cancellation Confirmation dialog box, click **OK** to confirm the cancellation.

Deleting Rendezvous Meetings

Users with the ADMIN or SYSTEM role can delete a Rendezvous meeting as long as there are no participants currently attending the meeting.

When you delete a Rendezvous meeting, the Cisco TelePresence Exchange System cancels the meeting if it has not been previously cancelled, frees up any ports of organization bandwidth or segments of guaranteed media bridge capacity associated with the meeting, and removes the meeting details and diagnostics.

To cancel the meeting without removing the details from the system, see the "Canceling Rendezvous Meetings" section on page 13-24.

Procedure

To delete a Rendezvous meeting, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 2 Click the applicable meeting to view the meeting details page.

Step 3 From the toolbar, click **Delete This Meeting**.

Note You cannot delete a meeting that is currently active.

Step 4 To confirm the cancellation and deletion, click **OK**.

Scheduling Rendezvous Meetings Fields

Table 13-8 Scheduling Rendezvous Meetings Fields

Field	Description
Basic Meeting Information	
Meeting Type	Radio buttons provide the following choices: • MeetMe—Scheduled meeting hosted by the local Cisco Telepresence Exchange System that provides the media bridge resources. Supports OBTP functionality. • Rendezvous—Timeless or reservationless meeting that is not limited by a single start time. Once created, a Rendezvous meeting starts whenever participants join the meeting. The local Cisco Telepresence Exchange System provides the media bridge resources. • Remote—Scheduled meeting hosted by a remote Cisco Telepresence Exchange System that provides the media bridge resources. Supports OBTP functionality. • Two Party Direct—Scheduled or ad-hoc meeting between two provisioned endpoints. The meeting does not require media bridge resources.
Subject	Text description of the meeting.
Service Provider	Drop-down list of service providers. Choose the service provider that will host this meeting.
Scheduler	Email address of the contact person for the meeting. When you enter this information, it is displayed on the telepresence IP phone during the meeting. This is useful if there is an issue with the meeting.
Scheduler's Organization	Drop-down list of the available organizations. Choose the organization of the scheduler to apply to the meeting. This field is required to enable service provider and organization inheritance capabilities. Some settings, such as automatic meeting extension and host settings, can be inherited. You can configure Meet-Me and Rendezvous meetings to inherit the settings from the meeting scheduler organization. Likewise, you can configure the organization to inherit the settings from the service provider. Service provider-level settings will be overridden if the inheritance option is not enabled at the organization level, and organization-level settings will be overridden if the inheritance option is not enabled at the meeting level. The scheduler organization is also used to determine the whitelist policy to apply to intra- and inter-service provider calls.
Reservation Type	Drop-down list of available reservation type names. Choose the name of the reservation type to apply to the meeting. The reservation type determines whether the system provides a guaranteed or best-effort level of service when reserving media bridge resources for the meeting. For more information about reservation types, see the "Configuring Reservation Types" section on page 13-46.

Table 13-8 Scheduling Rendezvous Meetings Fields (continued)

Field	Description
Maximum Meeting Instance Duration	Maximum length of any single instance of a Rendezvous meeting, in minutes, starting from the time the instance becomes active (when the first participant joins the meeting). The default value is 1440 minutes (24 hours). The range for the Rendezvous meeting is from 1 to 1440 minutes. An error occurs if the Rendezvous meeting exceeds 1440 minutes. At the end of the maximum meeting instance duration, all participants in the meeting are dropped, but participants can immediately rejoin the meeting as part of a new meeting instance.
Geographic Settings	
Region	Drop-down list of regions. Choose the region where the meeting will be hosted. The system reserves media resources at a media multi-region points of presence (POP) in this region. **Note** You cannot schedule a Meet-Me meeting or a Rendezvous meeting in the same region.
Service Number Name	Drop-down list of service number names. Choose the name of the service number that users dial to reach the service for the meeting.
Endpoint Provisioning Options	
Provisioned Endpoints	View only. This field is only editable when managing an active Rendezvous meeting. For information about managing active meetings, see the "Managing Active Meetings" section on page 13-32.
Unprovisioned Endpoints	View only. This field is only editable when managing an active Rendezvous meeting. For information about managing active meetings, see the "Managing Active Meetings" section on page 13-32.

Table 13-8 Scheduling Rendezvous Meetings Fields (continued)

Field	Description
Number of Endpoints	Specify the endpoint capacity to reserve for the meeting. To determine the capacity for the meeting, the system determines the type of media bridge resource to use for the meeting based on the profile(s) selected in the **Additional Media Profiles** field, multiplies the **Number of Endpoints** value by the default number of segments for that resource type, then adds the value in the **Additional Capacity** field. The default number of segments for a media bridge depends on the value of the **MeetMe Default Screens** parameter on the System > Global Configuration window, as follows: • CTMS—**MeetMe Default Screens** +1 • TPS—**MeetMe Default Screens** • MCU MSE 8510—1 segment, regardless of this value. To add additional capacity in a smaller multiple, use the **Additional Capacity** field. **Note** Because you cannot configure Provisioned Endpoints for a Rendezvous meeting, you must specify at least one additional media profile so that the system knows the type of bridge resource to allocate for the meeting. For more information on capacity reservation and bridge selection, see Appendix B, "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection."
Additional Media Profiles	Allows you to specify additional media profiles so that the system can choose the correct media bridge resource on which to reserve the meeting based on the capacity and capabilities required by unexpected or unspecified endpoints that may join the meeting. For example, if only CTS endpoints are added to a meeting, the system will try to reserve a CTMS resource for the meeting. If you add the built-in Default Generic H.323 media profile, then the system will try to reserve a TPS resource. **Note** You must specify at least one additional media profile so that the system knows the type of bridge resource to allocate for the meeting. To choose a media profile to include in the meeting, click **Add Media Profiles**.
Host/Guest Options	
Enable Host/Guest Roles	Check Box. Check this check box to enable host and guest options for the meeting.

Table 13-8 Scheduling Rendezvous Meetings Fields (continued)

Field	Description
Drop Participants On Host Exit	*Applicable only when Enable Host/Guest Roles is checked.* Radio buttons provide a choice of the following conditions. • False—The system does not drop any participants when the host leaves the meeting. • True—The system drops all participants from the meeting when the host leaves. If the meeting has more than one host, participants will be dropped when all hosts have left the meeting. • Inherit from Organization—Use the host/guest settings configured for the organization. **Note** You can configure the host settings at the service provider level, organization level, or meeting level. The policy is hierarchical, so you can configure a Meet-Me or Rendezvous meeting to inherit its settings from the meeting scheduler organization. In addition, you can configure an organization to inherit its settings from the service provider. If you want a meeting to inherit organization settings, you must enable the inheritance option at the meeting level. Similarly, if you want an organization to inherit service provider settings, you must enable the inheritance option at the organization level.
Host PIN	*Applicable only when Enable Host/Guest Roles is checked.* Radio buttons provide a choice of the following choices: • Auto-Generate—The system creates a host PIN that a participant must enter to join the meeting as a host. • Customize—The meeting scheduler specifies a custom host PIN that a participant must enter to join the meeting as a host.
Custom Host PIN	*Applicable only when Enable Host/Guest Roles is checked, and Customize is selected for the Host PIN.* The PIN that a participant must enter to join the meeting as a host.
Allowed Host Endpoints	List of the available endpoints that are designated as a host for the meeting. Only provisioned endpoints can be designated as a host. Click **Add Allowed Host Endpoint** to add an endpoint and configure the following values: • **Endpoint Organization**—Drop-down list of organizations that are associated with the Service Provider configured for the meeting. • **Endpoint Name**—Drop-down list of endpoints associated with the Endpoint Organization.

Table 13-8 Scheduling Rendezvous Meetings Fields (continued)

Field	Description
Advanced Options	
Additional Capacity	Number of additional media bridge resource segments to reserve for the meeting. **Note** A Rendezvous meeting does not have a restriction on the maximum value of the capacity. If the capacity is not available at attend time, the endpoints cannot join the meeting. Use this field to allocate media bridge resources for endpoints that are not configured to be part of the meeting but that you expect to join the meeting. To determine how many segments to add for each endpoint, use the following guidelines, depending on which media resource provides the meeting bridge: • Cisco TelePresence Multipoint Switch—Add 4 segments for each three-screen endpoint and 2 segments for each single-screen endpoint. • Cisco TelePresence Server MSE 8710—Add 3 segments for each three-screen endpoint and 1 segment for each single-screen endpoint. • Cisco TelePresence MCU MSE 8510—Add 1 segment. The MCU MSE 8510 supports only single-screen endpoints.
Conference ID	Text field. Enter a unique, eight-digit conference ID for users to dial to reach this meeting. **Note** The Conference ID is optional. If you do not enter an ID, the system will generate one for you.
Custom Screen Layout (Used on MSE 8510)	For meetings on the Cisco TelePresence Server MSE 8510, select the screen layout used to display participant video.

Meeting Details Fields for Rendezvous Meetings

Table 13-9 Meeting Details Field Descriptions for Rendezvous Meetings

Field	Description
Overview Tab	
Subject	Text description of the meeting.
Maximum Instance Duration	Maximum length of any single instance of the Rendezvous meeting, in minutes, starting from the time the instance becomes active (when the first participant joins the meeting).
Scheduler	Email address of the contact person for the meeting.
Service Provider	The service provider hosting the meeting.
Meeting Key	Unique identifier for the meeting. You can use the meeting key to identify this meeting in API requests.

Table 13-9 Meeting Details Field Descriptions for Rendezvous Meetings (continued)

Field	Description
Meeting Type	Indicates the type of meeting: MeetMe, Rendezvous, remote, or two-party direct. (In this case, Rendezvous.)
Cancelled	Indicates whether the meeting was cancelled. When you cancel a meeting, the system frees up any ports of organization bandwidth or segments of guaranteed media bridge capacity associated with the meeting, and participants can no longer join the meeting. After you cancel the meeting, the system continues to maintain the meeting details and diagnostics unless you delete the meeting.
Meet-Me Info Tab (Displayed only for meetings that have not been cancelled)	
Scheduler's Organization	Organization to which the meeting scheduler belongs. The scheduler organization is used to determine the whitelist policy to apply to intra- and inter-service provider calls. It is also used when the host and guest options feature is configured to inherit settings from the organization.
Remote Access Number	Number that users dial to reach the system when they dial in to the meeting.
Conference ID	Unique, eight-digit ID that users are prompted to enter when they dial in to the meeting.
Reserved Screens	Total number of segments of capacity that the system has reserved on the media bridge for the meeting. For Rendezvous meetings, the total is calculated based on the type of bridge on which the meeting will be hosted, the value in the Number of Endpoints field, and the value in the Additional Capacity field.
Region	Region of the media bridge resource that is hosting the meeting.
Large Meeting	Indicates whether the system classifies the meeting as a Large Meeting. Large meetings include 32 or more segments and are scheduled exclusively on media units that are reserved for large meetings.
Bridge Resource Type	Type of bridge that is hosting the meeting: CTMS (Cisco TelePresence Multipoint Switch), TPS (Cisco TelePresence Server MSE 8710), or TPS_8510 (Cisco TelePresence MCU MSE 8510).
Reservation Type	Reservation type specified for the meeting. The reservation type determines whether the meeting is guaranteed (the system reserved media bridge resources for the meeting when it was scheduled) or not guaranteed (the system did not reserve media bridge resources at scheduling time).
Host/Guest Roles Enabled	Indicates whether host and guest options are enabled.
Provisioned Endpoints Tab (Displayed only for active meetings that have provisioned endpoints configured)	
Endpoint	Cisco TelePresence Exchange System–provisioned name of the endpoint.
Ports	Number of segments of organization bandwidth that the endpoint requires. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.)
Minimize Capacity	Indicates whether the Minimize Capacity check box is checked on the organization to which the endpoint belongs.

Table 13-9 Meeting Details Field Descriptions for Rendezvous Meetings (continued)

Field	Description
Dialout	Indicates whether the system is configured to dial out to reach the endpoint.
Is Host	Indicates whether the endpoint is designated as a meeting host.
Organization	Organization to which the endpoint is associated.
Unprovisioned Endpoints Tab (Displayed only for active meetings that have unprovisioned endpoints configured)	
Ports	Number of segments of organization bandwidth that the endpoint requires. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.)
Organization	Organization to which the endpoint is associated.
Guest Dial Out	Indicates whether the system is configured to dial out to reach the endpoint.
Number	Phone number to dial to reach the endpoint (used if Guest Dial Out is true for the endpoint).
Media Profile	Media profile of the endpoint. When you add an unprovisioned endpoint to an active meeting, the system determines the protocol to use to dial out to the endpoint based on the protocols supported by the media profile and the type of bridge on which the meeting is hosted.
Allowed Host Endpoints Tab (Displayed only if host/guest roles are enabled and endpoints are configured as hosts)	
Endpoint Info	Cisco TelePresence Exchange System–provisioned name of the endpoint that is configured as a host for the meeting.

Managing Active Meetings

The Active Meetings page enables real-time management of Meet-Me and Rendezvous meetings that are currently in progress. The functions you can perform include locking or unlocking the meeting to control whether additional participants can join, muting or unmuting participants, increasing the media bridge resource capacity of the meeting, dialing out to endpoints, and increasing the duration of the meeting.

Note The Active Meetings page allows you to view and manage active Meet-Me and Rendezvous meetings only. You cannot use this page to actively manage remote and two-party direct meetings, because those meetings are not held on the Cisco TelePresence Exchange System–configured bridge resources (such as a Cisco TelePresence Multipoint Switch in the exchange).

The following sections describe how to use the Active Meetings page.

Prerequisites for Active Meeting Management

The following prerequisites apply to the use of active meeting management in the administration console only. See the *API User Guide for the Cisco TelePresence Exchange System Release 1.1* at http://www.cisco.com/en/US/products/ps11276/products_programming_reference_guides_list.html for requirements for the use of the active meeting management API.

- The active meeting management options are enabled only after you add a valid active meeting management (ActiveMeetingMgmt) feature license. For instructions, see "Managing Licenses" chapter.

  Without this license, you can only view the list of active meetings and view the diagnostic information of a given active meeting from the administration console, and you cannot make any changes to active meetings.

- You must log in to the administration console as a system, admin, or service desk user to use the active meeting management options. If you log in as any other user role, then you can only view the active meeting information and cannot make any changes to active meetings.

  The service desk user role is intended for users who schedule, modify or cancel meetings and manage active meetings. Users with this role have view-only access to other areas of the administration console.

Managing Active Meetings

Procedure

To manage an active Meet-Me or Rendezvous meeting, do the following procedure.

Step 1 Log in to the administration console as a system, admin, or service desk user.

Step 2 Click **Collaboration Services > Active Meetings.**

The page lists only currently active meetings and automatically refreshes as meetings become active and inactive.

See the "Field Reference for the Active Meetings List Page" section on page 13-34.

Step 3 To view a specific active meeting, click the meeting scheduler.

For help finding a specific meeting, see the "Sorting and Filtering Lists in the Administration Console" section on page 2-5.

Step 4 In the Active Meeting Control area, you can use the following options:

- **Lock Meeting** or **Unlock Meeting**—When locked, no more participants can join the meeting by dialing into the meeting. Unlocking a meeting allows participants to dial into the meeting. Dial-out endpoints are not affected by whether a meeting is locked or unlocked.
- **Unmute All Participants**—Unmutes any meeting participants that are currently muted.

Step 5 In the **Active Meeting Diagnostics** area, you can choose one of the following views:

- **Participants View**—The page automatically refreshes as participants join and leave the meeting. This view enables you to mute, unmute, drop, redial, and send text messages to display to specified participants. See the "Field Reference for the Participants View of Active Meeting Diagnostics" section on page 13-35.

Note When you check a check box to apply the mute, unmute, drop, redial or send text message action to a participant under the **Participants Joining or Currently in the Meeting** heading, wait for the "Updates Paused" message to display on the far right side of the heading bar before clicking the button to take the action. Occasionally, the page automatically refreshes before the "Updates Paused" message is displayed, which consequently clears your selection. If this happens, check the check box again, wait for the "Updates Paused" message, and then click the button to take the action

- **Events View**—Chronological summary of all events relating to this meeting that have occurred since the meeting was scheduled. For a Rendezvous meeting, this includes events from any previous instances of the meeting. See the "Field Reference for the Events View of Active Meeting Diagnostics" section on page 13-37.

Note Once a meeting ends or becomes inactive, all the change and control options for the meeting become disabled. You can, however, continue to view the diagnostic information for the meeting. Additional meeting event diagnostic information is also available by using Meeting Diagnostics. For more information, see the "Viewing Meeting Diagnostics for Active Meetings" section on page 25-7.

Step 6 (Optional) Select **Modify This Meeting** to make further changes to the meeting. See the "Field Reference for the Modify an Active Meeting Page" section on page 13-38.

Note On the meeting modification page, some settings are view-only when the meeting is active. For example, you cannot change the media bridge resource that is hosting the meeting, nor can you decrease the media bridge resource capacity of an active meeting. You can, however, increase the media bridge resource capacity of the meeting, dial out to additional endpoints, change host/guest settings, and increase the duration of the meeting.

Field Reference for the Active Meetings List Page

Table 13-10 Field Reference for the Active Meetings List Page

Field	Description
SUBJECT	Text description of the meeting. Click the subject to view the Meeting Diagnostics page for a specific active meeting.
SCHEDULER	Email address of the contact person for the meeting.
START TIME	Scheduled start time of the meeting or, in a Rendezvous meeting, the time when the first participant joined the meeting instance.

Table 13-10 Field Reference for the Active Meetings List Page (continued)

Field	Description
TIME REMAINING	How much time is left before the scheduled end time of the meeting. If the meeting has been extended past its scheduled end time, then this field shows the time remaining for the meeting extension. For a Rendezvous meeting, this field shows the time remaining for the meeting instance. Each Rendezvous meeting instance is limited by the Maximum Meeting Instance Duration for the meeting. If a Rendezvous meeting reaches the maximum meeting instance duration, all calls in that meeting will be dropped, but the participants can immediately rejoin the meeting.
CONFERENCE ID	The unique, eight-digit ID that users are prompted to enter if they dial in to the meeting rather than attending by using One-Button-to-Push (OBTP).
NUMBER OF PARTICIPANTS	How many participants are currently in the meeting.
CAPACITY (REMAINING/SCHEDULED)	Media bridge resource capacity, in segments. The first number shows how many segments are still available for the meeting. The second number shows how many segments were specified for the meeting when the meeting was scheduled. Each segment represents one screen of video transmission or one 30-fps data channel.
REGION	Region of the media bridge resource that is hosting the meeting. Click the region to view the region configuration details.
SCHEDULER ORGANIZATION	Organization to which the meeting scheduler belongs. The scheduler organization field is optional in some cases, and may not have been configured at the time the meeting was scheduled. Click the scheduler organization, if configured, to view the organization configuration details.

Field Reference for the Participants View of Active Meeting Diagnostics

Table 13-11 Field Reference for the Participants View of Active Meeting Diagnostics

Field	Description
Resources	
RESOURCE	Name of the media bridge resource that is hosting the meeting. Click the resource name to view the configuration details for the resource.
HOST	The IP address of the media bridge resource that is hosting the meeting. Click the host to open a new browser window to http://<*IP address of the media bridge resource*>.
REGION	Region of the media bridge resource that is hosting the meeting.

Table 13-11 Field Reference for the Participants View of Active Meeting Diagnostics (continued)

Field	Description
RESERVED CAPACITY	Media bridge resource capacity, in segments. Each segment represents one screen of video transmission or one 30-fps data channel. The RESERVED CAPACITY shows how many segments were reserved for the meeting. The AVAILABLE CAPACITY shows how many segments are still available for the meeting.
AVAILABLE CAPACITY	
STATIC MEETING ID	The meeting ID assigned for the meeting on the media bridge. This is called the static meeting identifier for CTMS and permanent meeting identifier for TPS and MCU MSE 8510, and falls within the range of values configured in the Vendor Config field on the configuration page for the media bridge.
Participants Joining or Currently in the Meeting	
PARTICIPANT	E.164 number or URI of the endpoint.
ENDPOINT NAME	Cisco TelePresence Exchange System–provisioned name of the endpoint. You can click the name to view the endpoint details. You may also see the following values: • Guest Endpoint—Dial-out guest endpoint. • Unprovisioned Endpoint—Dial-in unprovisioned endpoint.
JOIN TIME	When the participant joined the meeting.
CAPACITY USED	Number of media bridge resource segments that are utilized by the endpoint.
DIAL-IN/DIAL-OUT	One of the following values: • Requesting Dial-out—Cisco TelePresence Exchange System is requesting dial-out or will request dial-out when the host joins the meeting. • Connecting—MCU is attempting to connect to the endpoint. • Dial-out—MCU has connected to the dial-out endpoint. • Dial-in—Dial-in endpoint has connected to the MCU.
MUTE STATUS	Whether the participant is currently muted or unmuted.
DETAILS	Click the provided link to view details.
Drop	To use these options, first check the check box for one or more participants that are currently in the meeting. Then click the Drop, Mute, or Unmute button. **Note** If the meeting is hosted on a CTMS, selecting the mute option mutes the audio and video for the participant. If the meeting has only two participants, selecting the mute option mutes the audio and video for the participant and also places the other participant on hold. On a TPS and MSE 8510, selecting the mute option only mutes the audio for the participant.
Mute	
Unmute	

Table 13-11 Field Reference for the Participants View of Active Meeting Diagnostics (continued)

Field	Description
Send Endpoint Message	Sends text to display on one or more endpoints that are in the meeting. To use this option: 1. Check the check box for one or more participants that are currently in the meeting. 2. Enter the text that you want to display on the endpoints of the selected participants. 3. Click the Send Endpoint Message button. Restrictions: • The endpoint text display feature is not supported for meetings that are hosted on a Cisco TelePresence Multipoint Switch. • The message length cannot exceed 255 characters.
Previous Participants	
PARTICIPANT	E.164 number or URI of the endpoint.
ENDPOINT NAME	Cisco TelePresence Exchange System–provisioned name of the endpoint. You can click the name to view the endpoint details. You may also see the following values: • Guest Endpoint—Dial-out guest endpoint • Unprovisioned Endpoint—Dial-in unprovisioned endpoint
JOIN TIME	When the participant joined and left the meeting. This list also includes participants that tried but failed to join the meeting. For such entries, the join time is either empty or identical to the leave time.
LEAVE TIME	
CDR	Click the provided link to view details.
DETAILS	
Redial	To use this option, first check the check box for one or more participants that are not in the meeting. Then click **Redial**. The redial option is available only for dial-out participants.

Field Reference for the Events View of Active Meeting Diagnostics

Table 13-12 Field Reference for the Events View of Active Meeting Diagnostics

Field	Description
Meeting Events	
TIME	When the event occurred.
DESCRIPTION	Description of the event.
DETAILS	Click the provided link to view details.

Table 13-12 Field Reference for the Events View of Active Meeting Diagnostics (continued)

Field	Description
Alarms Near Meeting Time	
SEVERITY	Severity of the event message; one of the following values: • Emergency • Alert • Critical • Error • Warning • Notice • Info
TIME	When the alarm was generated.
SUMMARY	Description of the alarm.
SERVER	Server on which the alarm occurred.

Field Reference for the Modify an Active Meeting Page

Table 13-13 Field Reference for the Modify an Active Meeting Page

Field	Description
Basic Information	
Meeting Type	View only. Radio buttons provide a choice of MeetMe, Rendezvous, Remote, or Two Party Direct. • MeetMe meeting—The Cisco TelePresence Exchange System reserves media resources for the meeting. The meeting can include provisioned endpoints, unprovisioned endpoints, and remote endpoints. • Rendezvous—A meeting that does not have a preconfigured start time. Participants can join the meeting at any time. When one or more participants join a Rendezvous meeting, an instance of the meeting is created and the meeting is considered active. • Remote meeting—The local system does not reserve media resources for the meeting (the remote Cisco TelePresence Exchange System provides the media resources). A remote meeting involves an inter-service provider participant. • Two Party Direct—The system does not reserve media resources, because this type of meeting is direct-dialed. **Note** Only Meet-Me and Rendezvous meetings can be managed with active meeting management.
Subject	View only. Text description of the meeting.

Table 13-13 Field Reference for the Modify an Active Meeting Page (continued)

Field	Description
Start Time	View only. Scheduled start time of the meeting. **Note** This field is displayed only when managing a Meet-Me meeting.
Duration	Duration of the meeting in minutes. To increase the length of the meeting, enter a higher duration, up to a maximum of 1440 minutes (24 hours). For example, to add 30 minutes to a one-hour meeting, enter 90. **Note** This field is displayed only when managing a Meet-Me meeting.
Service Provider	View only. The service provider hosting the meeting.
Scheduler	View only. Email address of the contact person for the meeting.
Scheduler's Organization	Organization to which the meeting scheduler belongs. To change the scheduler organization, choose a new organization from the drop-down list. Changing the scheduler organization may change the whitelist policy that the system applies to intra-and inter-service provider calls, because the policy is based on the scheduler organization and the organization of the endpoint. Because you can configure certain settings (such as automatic meeting extension and meeting host settings) to inherit their values from the scheduler organization, changing the scheduler organization may also affect the values that the system uses for these settings. **Note** You can clear the scheduler organization by deleting the value in the Scheduler's Organization field. However, the system will not accept the change if the meeting has settings configured to inherit their values from the scheduler organization.
Reservation Type	View only. Reservation type specified for the meeting. The reservation type determines whether the meeting is guaranteed (the system reserved media bridge resources for the meeting when it was scheduled) or not guaranteed (the system did not reserve media bridge resources at scheduling time).
Maximum Meeting Instance Duration	View only. The maximum length of any single instance of a Rendezvous meeting, in minutes, starting from the point the instance becomes active (when one or more participants join the meeting). At the end of the maximum meeting instance duration, all calls in the meeting are dropped, but users can immediately rejoin the meeting as part of a new meeting instance. **Note** This field is displayed only when managing a Rendezvous meeting.
Geographic Settings	
Region	View only. Region of the media bridge resource that is hosting the meeting.
Service Number Name	View only. Name of the service number that users dial to reach the service for the meeting.

Table 13-13 Field Reference for the Modify an Active Meeting Page (continued)

Field	Description
Endpoint Provisioning Options	
Provisioned Endpoints	The provisioned endpoints that are currently attending the meeting. **Organization Name**—The organization to which the endpoint is associated. **Endpoint Name** —Name of an endpoint that is currently attending the meeting. **Ports** (displayed only when managing a Meet-Me meeting)—Number of segments of organization bandwidth that the endpoint requires. The default value is zero. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.) **Dial Out—**If the check box is checked, the system will dial out to reach the endpoint. When Dial Out is checked, you can click **Redial** on the Meeting Diagnostics page to have the system dial out to the endpoint again if the endpoint has left the meeting. This setting is view only for provisioned endpoints that are currently attending the meeting. **Is Host** (displayed only when managing a Meet-Me meeting)—If the check box is checked, the endpoint is designated as a host. Only provisioned endpoints can be designated as a host. This check box is view only for endpoints that are currently attending the meeting, and is used in conjunction with the Enable Host/Guest Roles check box.

Table 13-13 Field Reference for the Modify an Active Meeting Page (continued)

Field	Description
Add Provisioned Endpoint	Click **Add Provisioned Endpoint** and configure the following values. • **Endpoint Organization**—Drop-down list of organizations that are associated with the Service Provider configured for the meeting. • **Endpoint Name**—Drop-down list of endpoints associated with the Endpoint Organization. • **Ports** (displayed only when managing a Meet-Me meeting)—Enter the number of segments of organization bandwidth that the endpoint requires. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.) • **Dial Out**—Check this check box to have the system dial out to reach the endpoint. **Note** Any new endpoints added to a Rendezvous meeting will be automatically set to dial out. • **Host** (displayed only when managing a Meet-Me meeting)—Check the check box to designate the endpoint as a host. Only provisioned endpoints can be designated as a host. Use this check box in conjunction with the Enable Host/Guest Roles check box. To add an additional endpoint, click **Add Provisioned Endpoints** again. **Note** For Rendezvous meetings, the endpoint will be added only to the currently active instance of the meeting.

Table 13-13 Field Reference for the Modify an Active Meeting Page (continued)

Field	Description
Unprovisioned Endpoints	The unprovisioned endpoints that are currently attending the meeting. Unprovisioned endpoints reserve ports of bandwidth for an unknown endpoint for a specific organization. • **Bandwidth-Providing Organization**—Organization to which the endpoint belongs. • **Ports** (displayed only when managing a Meet-Me meeting)—Number of segments of organization bandwidth that the endpoint requires. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.) • **Guest Dial Out**—Indicates that the system will dial out to reach the endpoint. When Guest Dial Out is checked, you can click **Redial** on the Meeting Diagnostics page to have the system dial out to the endpoint again if the endpoint has left the meeting. This setting is view only for unprovisioned endpoints that are currently attending the meeting. • **Number**—Number that the system must dial to reach the endpoint. • **Media Profile**—At schedule time, the media profile helps tailor the bridge selection and capacity calculation to your needs. At attend time, the system determines the protocol to use when dialing out to the endpoint based on the protocols supported by the media profile and the type of bridge on which the meeting is hosted. For more information, see the "Protocol Used for Dial-Out Calls At Attend Time" section on page B-8.

Table 13-13 Field Reference for the Modify an Active Meeting Page (continued)

Field	Description
Add Unprovisioned Endpoint	Click **Add Unprovisioned Endpoints** to display a drop-down list of available organization names, and choose an organization to include in this meeting. • **Ports** (displayed only when managing a Meet-Me meeting)—Enter the number of segments of organization bandwidth that the endpoint requires. The default value is zero. (The Max Ports setting for the organization determines the sum total amount of bandwidth that the organization endpoints can consume at a given time.) • **Guest Dial Out**—Check this check box to have the system dial out to reach the endpoint. **Note** Any new endpoints added to a Rendezvous meeting will be automatically set to dial out. • **Number**—Enter the number that the system must dial to reach the guest endpoint. • **Media Profile**—Choose the media profile for the endpoint from the drop-down list. When you add an unprovisioned endpoint to an active meeting, the system determines the protocol to use to dial out to the endpoint based on the protocols supported by the media profile and the type of bridge on which the meeting is hosted. For more information, see the "Protocol Used for Dial-Out Calls At Attend Time" section on page B-8. To add an additional endpoint, click **Add Unprovisioned Endpoints** again. For Rendezvous meetings, the endpoint will be added only to the currently active instance of the meeting.
Remote Endpoints	Indicates whether capacity has been reserved for one or more remote endpoints for an inter-service provider participant. No additional data is visible for this type of endpoint. **Note** This field is displayed only when managing a Meet-Me meeting.
Add Remote Endpoint	To reserve capacity for a remote endpoint, click **Add Remote Endpoints**. A Remote Endpoint entry is displayed on the window. **Note** This field is displayed only when managing a Meet-Me meeting.

Table 13-13 Field Reference for the Modify an Active Meeting Page (continued)

Field	Description
Number of Endpoints	Specifies the endpoint capacity to reserve for the Rendezvous meeting. Modifying this value on the Modify an Active Meeting Page also changes the value for future instances of the meeting. For information on how many segments of bridge capacity the system reserves for an endpoint, see Appendix B, "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection." **Note** This field is displayed only when managing a Rendezvous meeting.
Additional Media Profiles	View only. Allows you to specify additional media profiles to so that the Cisco TelePresence Exchange System can choose the correct bridge resource type on which to reserve the meeting based on the capacity and capabilities required by unexpected or unspecified endpoints that may join the meeting. For example, if only CTS endpoints are added to a meeting, the system will try to reserve CTMS resources for the meeting. If an additional media profile is added for H.323, then the system will try to reserve a TPS resource.
Meeting Extension Options	
Meeting Extension	View only. Determines whether the meeting will be automatically extended if resources are available when the meeting nears the configured duration.
Meeting Extension Period (minutes)	*Available only if Meeting Extension was enabled before the meeting became active.* Specify the length to automatically extend the meeting by if resources are available when the meeting nears its configured duration. The extension length must be a multiple of 15 (for example, 15, 30 or 45). **Note** If you change the meeting extension period after the system has initiated an extension (starting shortly before the two minute end-of-meeting warning), the change will not take effect for the current extension. For example, on a meeting with two 15-minute extensions configured, if the system starts the first extension and you then change the Meeting Extension Period to 30 minutes, the first extension will remain 15 minutes. If the system is able to extend the meeting for the second extension, the second extension will be 30 minutes.
Max Meeting Extensions Allowed	*Available only if Meeting Extension was enabled before the meeting became active.* Specify the maximum number of times the meeting can be extended if resources are available. The maximum number of extensions times the Meeting Extension Period must not exceed 1440 minutes (24 hours).

Table 13-13 Field Reference for the Modify an Active Meeting Page (continued)

Field	Description
Host/Guest Options	
Enable Host/Guest Roles	Check box. Uncheck the check box during an active meeting to disable host and guest options for the meeting. **Note** You cannot use this field to enable host and guest options on an active meeting. In order for the options to be available for a meeting, you must enable the options before the meeting becomes active.
Drop Participants On Host Exit	*Applicable only when Enable Host/Guest Roles is checked.* View only. When checked, the system drops all participants from the meeting when the host leaves. If the meeting has more than one host, participants will be dropped when all hosts have left the meeting.
Host PIN	*Applicable only when Enable Host/Guest Roles is checked.* View only. Radio buttons provide the following choices: • Auto-Generate—The system creates a host PIN that a participant must enter to join the meeting as a host. • Customize—The meeting scheduler specifies a custom host PIN that a participant must enter to join the meeting as a host.
Custom Host PIN	*Applicable only when Enable Host/Guest Roles is checked, and Customize is selected for the Host PIN.* View only. The PIN that a participant must enter to join the meeting as a host.
Allowed Host Endpoints	*Applicable only when Enable Host/Guest Roles is checked for a Rendezvous meeting.* View only. List of the available endpoints that are designated as a host for the meeting, and the organization(s) with which they are associated. Only provisioned endpoints can be designated as a host.

Table 13-13 Field Reference for the Modify an Active Meeting Page (continued)

Field	Description
Advanced Options	
Additional Capacity	Number of additional media bridge resource segments to reserve for the meeting. Use this field to allocate media bridge resources for endpoints that are not configured to be part of the meeting but that you expect to join the meeting. To determine how many segments to add for each endpoint, use the following guidelines, depending on which media resource provides the meeting bridge: • Cisco TelePresence Multipoint Switch—Add 4 segments for each three-screen endpoint and 2 segments for each single-screen endpoint. • Cisco TelePresence Server MSE 8710—Add 3 segments for each three-screen endpoint and 1 segment for each single-screen endpoint. • Cisco TelePresence MCU MSE 8510—Add 1 segment. The MCU MSE 8510 supports only single-screen endpoints. **Note** For Rendezvous meetings, modifying this value on the Modify an Active Meeting Page also changes the value for future instances of the meeting. A Rendezvous meeting does not have a restriction on the maximum value of the capacity. If the capacity is not available at attend time, the endpoints cannot join the meeting.
Conference ID	View only. The unique, eight-digit ID that users are prompted to enter if they dial in to the meeting rather than attending by using One-Button-to-Push (OBTP).
Push OBTP	View only. Indicates whether the meeting was configured to send One-Button-to-Push (OBTP) information to the IP phones in the rooms that are associated with the provisioned endpoints. **Note** This field is displayed only when managing a Meet-Me meeting.
Custom Screen Layout (Used on MSE 8510)	For meetings on the Cisco TelePresence MCU MSE 8510, select the screen layout used to display participant video.
Cancel	To cancel any changes to the active meeting, click **Cancel**.
Schedule	To make changes to the active meeting, click **Schedule**.

Configuring Reservation Types

The reservation type determines whether the system provides a guaranteed or best-effort level of service when reserving media bridge resources for a Meet-Me or Rendezvous meeting. The reservation type levels of service are defined as follows:

- Guaranteed—When you create a guaranteed Meet-Me meeting, the system reserves media bridge resources for the specified meeting duration. For a guaranteed Rendezvous meeting, the system reserves resources for the meeting that can never be used for other meetings.
- Best-effort—When you create a best-effort Meet-Me or Rendezvous meeting, the system does not reserve any media bridge resources in advance for the meeting. Instead, the system allocates resources when the first participant joins the meeting and deallocates resources when the last participant leaves the meeting. For a best-effort meeting, the system may fail to allocate resources to the meeting because all the available resources may be in use by other best-effort meetings for the given time period.

You configure Meet-Me meetings, Rendezvous meetings, and resource groups to be associated with specific reservation types. When creating a resource group, you configure the allowable amount of dedicated media resources and meeting booking capacity for each reservation type chosen. Assigning both a guaranteed and best-effort reservation type to a single resource group allows you to dedicate a specific percentage of the resources to guaranteed meetings and another percentage to best-effort meetings.

For more information about how to configure resource groups, see the "Configuring Resource Groups" section on page 10-12.

The following sections describe how to configure reservation types:

Adding Reservation Types

Procedure

To add a new reservation type, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Reservation Types**.

The Reservation Types window is displayed.

Step 2 From the toolbar, click **Add A New Reservation Type**.

Step 3 Enter the fields as appropriate.

Table 13-14 describes the fields.

Step 4 To save your changes, click **Save**.

Editing Reservation Types

Procedure

To edit a reservation type, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Reservation Types**.

The Reservation Types window is displayed.

Step 2 In the item table, click the applicable entry.

A summary window for the reservation type is displayed.

Step 3 From the toolbar, click **Edit This Reservation Type**.

The Edit Reservation Type window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as appropriate.

Table 13-14 describes the fields.

Step 5 To save your changes, click **Save**.

Deleting Reservation Types

Before You Begin

To delete a reservation type, you need to remove all of the configuration items (such as meetings or resource groups) that are dependencies of this reservation type. For example, remove the reservation type that you want to delete from any associated resource groups, Rendezvous meetings or Meet-Me meetings that have not yet started. You cannot delete a reservation type that has been associated with a completed meeting.

Procedure

To delete a reservation type, do the following procedure:

Step 1 From the navigation pane, choose **Customers > Reservation Types**.

The Reservation Types window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple reservation types at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a reservation type prior to deleting it, in the Reservation Type window, you can click the applicable reservation type to go to the Reservation Type page. After verifying that you have chosen the correct reservation type to delete, click **Delete This Reservation Type** in the toolbar, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Note When a dependency exists, the delete operation aborts and an error message is displayed that describes the dependent configuration item.

Reservation Type Fields

Table 13-14 Reservation Type Field Descriptions

Field	Description
Name	Text string identifying this reservation type. See the "Common Field Properties" section on page 2-4.
Description	Text string describing this reservation type. See the "Common Field Properties" section on page 2-4.
Guaranteed	Check box. When you check this check box, meetings that are assigned this reservation type will be created as a guaranteed meeting. If you do not check the check box, meetings will be created as a best-effort meeting. **Note** Cisco recommends that you avoid changing an existing reservation type from guaranteed to best-effort. This type of change may cause meetings configured with the original guaranteed reservation type to fail. For additional information about guaranteed and best-effort meetings, see the "Configuring Reservation Types" section on page 13-46.

CHAPTER 14

Managing Licenses

The administration console provides the ability to upload license files to the Cisco TelePresence Exchange System and to view the status of licenses. The following sections describe how to manage licenses:

Viewing Licenses

Procedure

To view the status of Cisco TelePresence Exchange System licenses, do the following procedure:

Step 1 From the navigation pane, choose **Licensing > License Files**.

The License Files window is displayed.

Step 2 To view details for a specific license, click the name of the license.

Step 3 (Optional) To filter on the entries in the license listing, do one of the following:

- To filter by the name of the license file name, click the **T** icon in that column and then enter the file name in the panel that appears. Click **Filter**.

  Click **Cancel** in the panel to clear the defined filter.
- To filter by the installation date of the license file name, click the **T** icon in that column and then enter a start and end date in the panel that appears. Click **Filter**.

  Click **Cancel** in the panel to clear the defined filter.

Step 4 (Optional) To clear all defined filters (name and installation date), click **Clear Filters** (on the right side of the page).

Uploading Licenses

Procedure

To upload licenses to the Cisco TelePresence Exchange System, do the following procedure:

Step 1 From the navigation pane, choose **Licensing > License Files**.

The License Files window is displayed.

Step 2 To select the license file, click **Browse**.

The Choose File to Upload or File Upload window opens depending on the browser that you are using.

Step 3 Browse to the folder containing the license file, then select the license file.

Step 4 To upload the license file, click **Open**.

Step 5 To ensure the file uploads successfully, click **Verify**.

PART 4

Configuring External Network Components for Cisco TelePresence Exchange System

CHAPTER 15

Configuring the Cisco Application Control Engine

The following sections describe how to configure the Cisco Application Control Engine:

About the Cisco Application Control Engine

This section describes the Cisco Application Control Engine (ACE) and includes the following topics:

ACE Overview

The ACE provides access control, load balancing, and high availability functionality for the Cisco TelePresence Exchange System server cluster.

Clients gain access to the server cluster through the ACE. The ACE provides a virtual IP address (VIP) that acts as a proxy for the servers. The ACE distributes client requests to the servers based on the service requested, the load-balancing algorithm, the health of the servers, and session persistence requirements.

The ACE distributes the following types of incoming Cisco TelePresence Exchange System traffic:

- SIP traffic to the call engines
- HTTP traffic to the IVR application on the call engines
- HTTP traffic to the administration servers

ACE Topology

You can configure up to four interfaces on the ACE appliance.

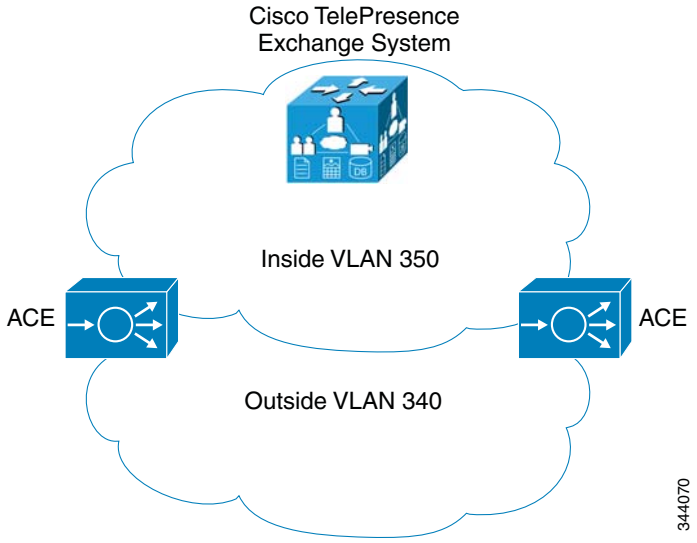
- You must configure one interface to serve as the outside interface.

  The outside interface connects to the users of the Cisco TelePresence Exchange System cluster.

If you have a redundant ACE in the application, you must configure the outside interface as a trunk to support both a native VLAN for untagged traffic, and a fault tolerant (FT) VLAN to provide a communication path between the two ACE appliances. The two ACE appliances are in an active/standby configuration. The ACE in standby is known as the peer.

- You must configure one interface to serve as the inside interface to provide access to the Cisco TelePresence Exchange System.

Note The inside and outside interfaces must belong to different VLANs.



Configuration Overview

The ACE appliance provides server load balancing for three types of message traffic:

- SIP call control
- HTTP messages for the IVR service
- HTTP messages for the administration console

To configure the ACE for the Cisco TelePresence Exchange System, complete the following procedures:

Note For links to the ACE configuration procedures listed below, see the "Configuring the Cisco Application Control Engine" section on page 15-4.

1. Configure the hostname.
2. Configure the physical interfaces.

   Assign VLANs to the interfaces.
3. Configure the real servers.

   Create a real server for each server in the Cisco TelePresence Exchange System cluster.
4. Configure access control lists.

Create access control lists (ACLs) to filter incoming or outgoing traffic on an interface based on configurable criteria (such as protocol type or IP address ranges).

5. Configure health probes.

   Create a health probe for each traffic type supported by Cisco TelePresence Exchange System. A health probe defines the type of message that the ACE will periodically send to the servers, and the expected responses.

6. Configure the server farms.

   Create a server farm for each Cisco TelePresence Exchange System traffic type. A server farm is a virtual server that provides a specific service. The ACE load-balances the incoming requests among the real servers that are associated with the server farm. The ACE also monitors server health (by sending periodic probes) and distributes work only to the operational real servers.

7. Configure session persistence.

   Create a sticky group for each server farm. A sticky group defines how to identify the session that is associated with each incoming message.

8. Configure a management class map and a policy map.

   Create these policies to allow remote management access to the Cisco TelePresence Exchange System cluster.

9. Configure Layer 7 load balancing policy maps and class maps.

   Define Layer 7 policy maps and class maps for each of the three traffic types. Layer 7 class maps and policy maps define the classification and policy for traffic based on upper-layer message parameters such as HTTP header fields and SIP header fields.

10. Configure Layer 3 and Layer 4 policy maps and class maps.

    Define Layer 3 and Layer 4 policy maps and class maps for each of the three traffic types. These class maps and policy maps define the classification and policy for traffic based on Layer 3 and Layer 4 message parameters such as source IP address, port, and protocol.

    Each Layer 7 policy must be included in a Layer 3 and Layer 4 policy.

11. Configure VLAN interfaces.

    Activate the management and load-balancing policies by associating the policy maps with the VLAN interfaces.

12. Configure miscellaneous ACE parameters and logging options.

    Configure various parameters and settings that are important for correct operation of the Cisco TelePresence Exchange System.

An overview of the ACE appliance is available in the *Cisco ACE 4700 Series Application Control Engine Appliance Quick Start Guide*, at http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA3_2_2/configuration/quick/guide/ace_appliance_qsg.html.

Additional information about ACE appliance configuration for server load balancing is available in the *Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide*, at http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA4_2_0/configuration/slb/guide/slbgd.html.

Additional information about configuring redundant ACE appliances is available in the *Cisco ACE 4700 Series Appliance Administration Guide*, at http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA4_2_0/configuration/administration/guide/redundcy.html.

Other documents related to the ACE appliance are available at http://www.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html.

Configuring the Cisco Application Control Engine

This section describes how to configure the ACE and includes the following topics:

Note All IP addresses shown in the configurations are for example purposes only.

Configuring the Hostname

By default the hostname of the ACE is switch. You can assign a specific name to the ACE. For configurations in which a redundant pair of ACEs is in use, you need to define both a hostname for the primary ACE (active system) and a peer hostname for the standby system.

All configuration for the ACE is done on the primary ACE. All configuration and changes in status are regularly communicated to the standby ACE through the fault-tolerant VLAN.

To configure the hostname for the ACE, do the following task:

	Command	Purpose
Step 1	`switch/Admin# configure terminal`	Enters configuration mode.
Step 2	`switch/Admin(config)# peer hostname` *name*	Configures the hostname for the peer (standby) ACE. The active ACE regularly communicates its configuration to the peer ACE. (Required only for redundant ACE configuration). The hostname is a case-sensitive text string from 1 to 32 alphanumeric characters in length. The default value of hostname is **switch**.

	Command	Purpose
Step 3	`switch/Admin(config)#` **`hostname`** *`name`*	Configures the hostname for the active ACE.
Step 4	`hostname/Admin(config)#` **`exit`**	Exits configuration mode.

The following example shows how to set the hostname for an ACE in a non-redundant configuration to ACE_1:

```
switch/Admin# configure terminal
switch/Admin(config)# hostname ACE_1
ACE_1/Admin(config)# exit
```

The following example shows how to set hostnames for two ACEs in a redundant configuration where ACE_1 is the active ACE and ACE_2 is the peer ACE that is in standby:

```
switch/Admin# configure terminal
switch/Admin(config)# peer hostname ACE_2
switch/Admin(config)# hostname ACE_1
ACE_1/Admin(config)# exit
```

Configuring Interfaces

You can configure up to four interfaces on the ACE. You must configure at least one outside interface and one inside interface. The outside interface connects to the users of the Cisco TelePresence Exchange System server cluster and the inside interface connects to the server cluster.

The inside and outside interfaces must belong to different VLANs.

To configure an interface on the ACE, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin#` **`configure terminal`**	Enters configuration mode.
Step 2	`ACE_1/Admin(config)#` **`interface gigabitEthernet`** *`slot_number / port_number`*	Enters interface configuration mode to define the first interface.
Step 3	`ACE_1/Admin(config-if)#` **`switchport access vlan`** *`vlan_ID`*	Assigns an access VLAN to the interface. When this is a new VLAN, the VLAN interface is automatically created.
Step 4	`ACE_1/Admin(config-if)#` **`no shutdown`**	Enables the first interface.
Step 5	`ACE_1/Admin(config)#` **`interface gigabitEthernet`** *`slot_number / port_number`*	Defines a second interface.
Step 6	`ACE_1/Admin(config-if)#` **`speed 1000`**	Assigns a speed of 1000Mbps to the interface. (Required only for the redundant ACE configuration).
Step 7	`ACE_1/Admin(config-if)#` **`duplex full`**	Assigns full-duplex mode to the interface. (Required only for the redundant ACE configuration).

	Command	Purpose
Step 8	`ACE_1/Admin(config-if)# carrier-delay {down milliseconds [up milliseconds]| up milliseconds [down milliseconds]}`	Delays the processing of hardware link down and link up notifications. Delay values are in ms. (Required only for the redundant ACE configuration).
Step 9	`ACE_1/Admin(config-if)# qos trust cos`	Sets the trusted state of an interface by defining which packet classifications the interface can carry. Definable classifications are CoS, ToS, and DSCP. (Required only for the redundant ACE configuration).
Step 10	`ACE_1/Admin(config-if)# switchport trunk native vlan vlan_ID`	Assigns a native trunk VLAN to the interface for untagged traffic. (Required for redundant ACE configurations.)
Step 11	`ACE_1/Admin(config-if)# switchport trunk allowed vlan vlan_ID`	Assigns a VLAN to the interface that can receive and transmit traffic on the trunk. You can define multiple VLANs on this trunk. In redundant ACE configurations, you define a fault-tolerant VLAN to provide a communication path for the heartbeat between the redundant ACE pair, in addition to a native VLAN. (Required for redundant ACE configurations.)
Step 12	`ACE_1/Admin(config-if)# no shutdown`	Enables the interface.
Step 13	`ACE_1/Admin(config)# interface gigabitEthernet slot_number / port_number`	Enters interface configuration mode to define the third interface.
Step 14	`ACE_1/Admin(config-if)# switchport access vlan vlan_ID`	Assigns an access VLAN to the interface.
Step 15	`ACE_1/Admin(config-if)# no shutdown`	Enables the interface. **Note** Repeat steps 13 through 15 to define the fourth interface.
Step 16	`ACE_1/Admin(config-if)# exit`	Exits interface configuration mode.

Non-Redundant Configuration

The following example shows how to configure and enable port 1 as the inside interface and port 2 as the outside interface for a non-redundant ACE configuration:

Interfaces 3 and 4 are not configured or enabled in this configuration and instead are shut down.

```
ACE_1/Admin# config
ACE_1/Admin(config)# interface gigabitEthernet 1/1
ACE_1/Admin(config-if)# switchport access vlan 350
ACE_1/Admin(config-if)# no shutdown

ACE_1/Admin(config)# interface gigabitEthernet 1/2
ACE_1/Admin(config-if)# switchport access vlan 340
ACE_1/Admin(config-if)# no shutdown

ACE_1/Admin(config)# interface gigabitEthernet 1/3
ACE_1/Admin(config-if)# shutdown

ACE_1/Admin(config)# interface gigabitEthernet 1/4
ACE_1/Admin(config-if)# shutdown
ACE_1/Admin(config-if)# exit
```

Redundant Configuration

The following example shows how to configure port 1 as the inside interface and port 2 as the outside trunk interface and ports 3 and 4 as access interfaces in a redundant ACE configuration:

```
ACE_1/Admin# config
ACE_1/Admin(config)# interface gigabitEthernet 1/1
ACE_1/Admin(config-if)# switchport access vlan 350
ACE_1/Admin(config-if)# no shutdown

ACE_1/Admin(config)# interface gigabitEthernet 1/2
ACE_1/Admin(config-if)# speed 1000
ACE_1/Admin(config-if)# duplex full
ACE_1/Admin(config-if)# carrier-delay down 30 up 30
ACE_1/Admin(config-if)# switchport trunk native vlan 340
ACE_1/Admin(config-if)# switchport trunk allowed vlan 340, 999
ACE_1/Admin(config-if)# no shutdown

ACE_1/Admin(config)# interface gigabitEthernet 1/3
ACE_1/Admin(config-if)# switchport access vlan 390
ACE_1/Admin(config-if)# no shutdown

ACE_1/Admin(config)# interface gigabitEthernet 1/4
ACE_1/Admin(config-if)# switchport access vlan 410
ACE_1/Admin(config-if)# no shutdown
ACE_1/Admin(config-if)# exit
```

Configuring Real Servers

Configure a real server for each physical administration and call engine server in the cluster.

To configure a real server, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)# rserver name`	Enters real server configuration mode for the specified real server.
Step 2	`ACE_1/Admin(config-rserver-host)# ip address ip_address`	Configures the IP address for the real server.
Step 3	`ACE_1/Admin(config-rserver-host)# inservice`	Places the real server in-service.
Step 4	`ACE_1/Admin(config-rserver-host)# exit`	Exits real server configuration mode.

The following example shows how to configure the administration real servers:

```
ACE_1/Admin(config)# rserver CTX-ADMIN-1
ACE_1/Admin(config-rserver-host)# ip address 10.22.139.123
ACE_1/Admin(config-rserver-host)# inservice
ACE_1/Admin(config-rserver-host)# exit
ACE_1/Admin(config)# rserver CTX-ADMIN-2
ACE_1/Admin(config-rserver-host)# ip address 10.22.139.124
ACE_1/Admin(config-rserver-host)# inservice
ACE_1/Admin(config-rserver-host)# exit
```

The following example shows how to configure the call engine real servers:

```
ACE_1/Admin(config)# rserver SIPE-1
ACE_1/Admin(config-rserver-host)# ip address 10.22.139.125
ACE_1/Admin(config-rserver-host)# inservice
ACE_1/Admin(config-rserver-host)# exit
ACE_1/Admin(config)# rserver SIPE-2
ACE_1/Admin(config-rserver-host)# ip address 10.22.139.126
ACE_1/Admin(config-rserver-host)# inservice
ACE_1/Admin(config-rserver-host)# exit
ACE_1/Admin(config)#
```

Configuring Access Control Lists

Access control lists (ACLs) allow you to filter incoming or outgoing traffic on an interface based on configurable criteria (such as protocol type or IP address ranges).

For the Cisco TelePresence Exchange System, configure an ACL to permit all IP traffic from any source address to any destination address. To create the ACL, enter the following command in configuration mode:

```
ACE_1/Admin(config)# access-list ALL line 8 extended permit ip any any
```

Configuring Health Probes

You can configure health probes to monitor the health of the Cisco TelePresence Exchange System server cluster. The ACE appliance periodically sends a probe message to each server and evaluates the response to determine the state of the server.

The following sections describe the health probes that you can configure for the server cluster:

- Configuring an HTTP Health Probe, page 15-8
- Configuring a SIP Health Probe, page 15-9

Configuring an HTTP Health Probe

You can configure HTTP health probes to monitor the IVR application on the call engines and the administration console on the administration servers.

To configure an HTTP health probe, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)# probe http` *probe_name*	Creates an HTTP probe with the specified name and enters HTTP probe configuration mode.
Step 2	`ACE_1/Admin(config-probe-http)#` **port** *port-number*	Configures the destination port number to use for the probe.
Step 3	`ACE_1/Admin(config-probe-http)#` **interval** *seconds*	Configures the time interval between probes (in seconds). The default value is 15 seconds.
Step 4	`ACE_1/Admin(config-probe-http)#` **faildetect** *retry-count*	Configures the number of consecutive failed probes before the server state is marked as failed. The default value is 2.
Step 5	`ACE_1/Admin(config-probe-http)#` **passdetect interval** *seconds*	Configures the time interval (in seconds) between sending probes to a failed server.

	Command	Purpose
Step 6	`ACE_1/Admin(config-probe-http)# request method get [ url url_string ]`	Configures the probe to use the HTTP GET method to get the page for the specified universal resource locator (URL). The default value for the URL is forward slash. **Note** Use **Ctrl+V** to escape special characters in the CLI, such as question mark (?). For example, type **HttpPing[Ctrl+V]?healthCheck** to enter **HttpPing?healthCheck** in the configuration.
Step 7	`ACE_1/Admin(config-probe-http)# expect status min_number max_number`	Configures the range (minimum and maximum values) of HTTP status codes that an ACE expects in the probe response. To configure a single status code, enter the same number for min_value and max_value.
Step 8	`ACE_1/Admin(config-probe-http)# open timeout`	Configures the time interval (in seconds) to wait for a TCP connection to be established. By default, the ACE waits 10 seconds to open and establish the connection with the server.

The following example shows how to configure the HTTP health probe for the administration server:

```
ACE_1/Admin(config)# probe http ctx-admin
ACE_1/Admin(config-probe-http)# port 8080
ACE_1/Admin(config-probe-http)# interval 2
ACE_1/Admin(config-probe-http)# faildetect 2
ACE_1/Admin(config-probe-http)# passdetect interval 4
ACE_1/Admin(config-probe-http)# request method get url /ctxadmin/ping
ACE_1/Admin(config-probe-http)# expect status 200 200
ACE_1/Admin(config-probe-http)# open 1
```

The following example shows how to configure the HTTP health probe for the IVR application on the call engines:

```
ACE_1/Admin(config)# probe http IVR
ACE_1/Admin(config-probe-http)# port 8080
ACE_1/Admin(config-probe-http)# interval 5
ACE_1/Admin(config-probe-http)# faildetect 2
ACE_1/Admin(config-probe-http)# passdetect interval 4
ACE_1/Admin(config-probe-http)# request method get url /MeetMePing/HttpPing?healthCheck=true
ACE_1/Admin(config-probe-http)# expect status 200 200
ACE_1/Admin(config-probe-http)# open 1
```

Configuring a SIP Health Probe

You can define SIP (UDP and TCP) probes to monitor the health of the call processing service.

To configure a SIP health probe, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)# probe sip {udp | tcp} name`	Enter the type of SIP probe (UDP or TCP) and the name of the probe.
Step 2	`ACE_1/Admin(config-probe-sip)# interval seconds`	Configures the time interval between probes (in seconds). The default value is 15 seconds.
Step 3	`ACE_1/Admin(config-probe-sip)# faildetect retry-count`	Configures the number of consecutive failed probes before the server state is marked as failed. The default value is 2.

	Command	Purpose
Step 4	`ACE_1/Admin(config-probe-sip)#` **`passdetect interval`** *`seconds`*	Configures the time interval (in seconds) between sending probes to a failed server, or the number of consecutive successful probe responses before marking the server state as active.
Step 5	`ACE_1/Admin(config-probe-sip)#` **`passdetect count`** *`number`*	Configures the number of consecutive successful probe responses before marking the server state as active.
Step 6	`ACE_1/Admin(config-probe-sip)#` **`expect status`** *`min_number max_number`*	Configures the range (minimum and maximum values) of status codes that an ACE expects in the probe response. To configure a single status code, enter the same number for min_value and max_value.
Step 7	`ACE_1/Admin(config-probe-sip)#` **`open`** *`timeout`*	Configures the time interval (in seconds) to wait for a TCP connection to be established. By default, the ACE waits 10 seconds to open and establish the connection with the server.

The following example shows how to configure a SIP UDP probe:

```
ACE_1/Admin(config)# probe sip udp SIP-OPTION
ACE_1/Admin(config-probe-sip)# interval 2
ACE_1/Admin(config-probe-sip)# faildetect 1
ACE_1/Admin(config-probe-sip)# passdetect interval 4
ACE_1/Admin(config-probe-sip)# passdetect count 2
ACE_1/Admin(config-probe-sip)# expect status 200 200
ACE_1/Admin(config-probe-sip)# open 1
```

The following example shows how to configure a SIP TCP probe:

```
ACE_1/Admin(config)# probe sip tcp SIP-TCP-OPTION
ACE_1/Admin(config-probe-sip)# interval 2
ACE_1/Admin(config-probe-sip)# faildetect 1
ACE_1/Admin(config-probe-sip)# passdetect interval 4
ACE_1/Admin(config-probe-sip)# passdetect count 2
ACE_1/Admin(config-probe-http)# expect status 200 200
ACE_1/Admin(config-probe-http)# open 1
```

Creating Server Farms

A server farm is a connected group of real servers that perform the same function. You must define at least two real servers to include in a server farm.

To create a server farm and define real server membership for those server farms, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)#` **`serverfarm host`** *`name`*	Creates the server farm and enters the server farm configuration mode for the specified server farm.
Step 2	`ACE_1/Admin(config-sfarm-host)#` **`failaction purge`**	Configures the action that is taken if a real server in the server farm goes down. Purge indicates that ACE removes the connection to the real server and sends a reset (RST) to the server.
Step 3	`ACE_1/Admin(config-sfarm-host)#` **`probe`** *`name`*	Specifies the probe to use for monitoring the health of real servers in this server farm.
Step 4	`ACE_1/Admin(config-sfarm-host)#` **`rserver`** *`name`*	Associates the specified real server as a member of this server farm.

	Command	Purpose
Step 5	`ACE_1/Admin(config-sfarm-host-rs)# inservice`	Places the real server in service.
Step 6	`ACE_1/Admin(config-sfarm-host-rs)# exit`	Exits server farm real-server configuration mode
Step 7	`ACE_1/Admin(config-sfarm-host)# exit`	Exits server farm configuration mode.

For the Cisco TelePresence Exchange System:

- Create a server farm for the administration console service and associate at least two administration servers (on which the administration console runs) to the server farm.
- Create a server farm for the IVR application and associate at least two call engine servers (on which the IVR application runs) to the server farm.
- Create a server farm for the SIP (call processing) service and associate at least two call engine servers (on which the SIP service runs) to the server farm.

Real servers can belong to multiple server farms. Although the SIP service and IVR application both run on the call engine (real server), you define a separate server farm for each service because the health probes and the session persistence criteria are different for the two services.

The following example shows how to configure a server farm for the administration console on the administration servers:

```
ACE_1/Admin(config)# serverfarm host CTX-ADMIN
ACE_1/Admin(config-sfarm-host)# failaction purge
ACE_1/Admin(config-sfarm-host)# probe ctx-admin
ACE_1/Admin(config-sfarm-host)# rserver CTX-ADMIN-1
ACE_1/Admin(config-sfarm-host-rs)# inservice
ACE_1/Admin(config-sfarm-host-rs)# exit
ACE_1/Admin(config-sfarm-host)# rserver CTX-ADMIN-2
ACE_1/Admin(config-sfarm-host-rs)# inservice
ACE_1/Admin(config-sfarm-host-rs)# exit
```

The following example shows how to configure a server farm for the IVR application on the call engine servers:

```
ACE_1/Admin(config)# serverfarm host IVR_SERVERS
ACE_1/Admin(config-sfarm-host)# failaction purge
ACE_1/Admin(config-sfarm-host)# probe IVR
ACE_1/Admin(config-sfarm-host)# rserver SIPE-1
ACE_1/Admin(config-sfarm-host-rs)# inservice
ACE_1/Admin(config-sfarm-host-rs)# exit
ACE_1/Admin(config-sfarm-host)# rserver SIPE-2
ACE_1/Admin(config-sfarm-host-rs)# inservice
ACE_1/Admin(config-sfarm-host-rs)# exit
```

The following example shows how to create a server farm for the SIP service on the call engine servers:

```
ACE_1/Admin(config)# serverfarm host SIP_FARM
ACE_1/Admin(config-sfarm-host)# failaction reassign
ACE_1/Admin(config-sfarm-host)# probe SIP_UDP-OPTION
ACE_1/Admin(config-sfarm-host)# rserver SIPE-1
ACE_1/Admin(config-sfarm-host-rs)# inservice
ACE_1/Admin(config-sfarm-host-rs)# exit
ACE_1/Admin(config-sfarm-host)# rserver SIPE-2
ACE_1/Admin(config-sfarm-host-rs)# inservice
ACE_1/Admin(config-sfarm-host-rs)# exit
```

Configuring Session Persistence

Session persistence ensures that the system directs all messages for a session to the same real server. Session persistence is also known as stickiness.

On the ACE, you configure session persistence by defining sticky groups. The sticky group defines how to identify sessions based on the value of specific fields within the incoming messages.

For the Cisco TelePresence Exchange System, configure a sticky group for each of the server farms.

This section addresses sticky group configuration and includes the following topics:

Creating SIP Header Sticky Groups

The SIP header sticky group identifies sessions based on fields in the SIP message header.

For the call processing service, create a sticky group based on the SIP Call ID field. All messages with the same call ID will be directed to the same real server.

To create a SIP header sticky group, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)# sticky sip-header Call-ID name2`	Creates a SIP header sticky group, which recognizes sessions based on the Call ID field in the header.
Step 2	`ACE_1/Admin(config-sticky-header)# timeout minutes`	Configures a timeout value for the sticky group. The value is the number of minutes that the ACE retains the sticky information for each client session. The default value is 1440 minutes.
Step 3	`ACE_1/Admin(config-sticky-header)# serverfarm name1`	Associates a server farm with this sticky group.

The following example shows how to create a sticky group that uses the SIP call ID field to identify sessions:

```
ACE_1/Admin(config)# sticky sip-header Call-ID SIP_FARM
ACE_1/Admin(config-sticky-header)# timeout 5
ACE_1/Admin(config-sticky-cookie)# serverfarm SIP_FARM
```

Creating HTTP Cookie Sticky Groups

The HTTP cookie sticky group identifies sessions based on the cookie value in the HTTP header. The system directs all messages with the same cookie value to the same server. The ACE can insert a cookie into the server response for the first client message. The ACE uses this cookie value to identify the session, and then forwards this same cookie value in all subsequent client messages.

To create the HTTP cookie sticky group, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)# sticky http-cookie name1 name2`	Creates an HTTP cookie sticky group, which recognizes sessions based on the cookie value (name1) in the HTTP header. Name2 is the name of the sticky group.
Step 2	`ACE_1/Admin(config-sticky-cookie)# cookie insert browser-expire name`	Enables cookie insertion. The ACE inserts a session cookie in the server response to the client, to ensure stickiness to the same server. Browser-expire allows the client browser to expire the cookie after the session ends.
Step 3	`ACE_1/Admin(config-sticky-cookie)# serverfarm name`	Associates the sticky group with the specified SIP server farm.

The following example shows how to configure an HTTP cookie sticky group for the administration console:

```
ACE_1/Admin(config)# sticky http-cookie ctx_1 WEB_STICKY
ACE_1/Admin(config-sticky-cookie)# cookie insert browser-expire
ACE_1/Admin(config-sticky-cookie)# serverfarm CTX-ADMIN
```

Creating HTTP Header Sticky Groups

The HTTP header sticky group identifies sessions based on the value of fields in the HTTP header. You can configure the sticky group to use a specific portion of the header.

To create an HTTP header sticky group, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)# sticky http-header name1 name2`	Creates an HTTP header sticky group. Name1 is the HTTP header name. Name2 is the name of the sticky group.
Step 2	`ACE_1/Admin(config-sticky-header)# header offset number1 [ length number2 ]`	The header offset specifies how many bytes to ignore (starting from the first byte of the header). Length specifies the number of bytes of header that the ACE uses to identify the session.
Step 3	`ACE_1/Admin(config-sticky-header)# serverfarm name`	Associates the sticky group with the specified SIP server farm.

The following example shows how to define an HTTP header sticky group for the IVR application:

```
ACE_1/Admin(config)# sticky http-header Host IVR_STICKY
ACE_1/Admin(config-sticky-header)# header offset 0 length 0
ACE_1/Admin(config-sticky-header)# serverfarm IVR_SERVERS
```

Configuring Class Maps

A Layer 3 and Layer 4 class map classifies traffic based on the Layer 3 and Layer 4 information (such as IP address, IP protocol, or port number). A Layer 7 class map classifies traffic based on fields in the upper-layer protocols (such as HTTP or SIP). A management class map classifies traffic based on management protocols (such as ICMP, SNMP, SSH, or Telnet).

This section addresses configuration for class maps and includes the following topics:

Configuring Layer 7 HTTP Class Maps

To create a Layer 7 class map for server load balancing based on the URL value in the HTTP header, do the following task:

	Command	Purpose
Step 1	ACE_1/Admin(config)# **class-map type http loadbalance match-any** *map_name*	Creates a Layer 7 class map for HTTP server load balancing. The match-any keyword indicates that a message matches this class map if any of the configured match statements are true. The name has a maximum of 64 alphanumeric characters and must not contain spaces.
Step 2	ACE_1/Admin(config-cmap-http-lb)# [*line_number*]**match http url** *expression* [**method** *name*]	Configures a URL (or portion of a URL) to match when making the load-balancing decision. The optional method keyword specifies the HTTP 1.1 method name to include in the match.
Step 3	ACE_1/Admin(config-cmap-http-lb) **exit**	Exits the class map HTTP load balancing configuration mode.

The following example shows how to create a class map for Layer 7 load balancing of HTTP traffic to the IVR application:

```
ACE_1/Admin(config)# class-map type http loadbalance match-any IVR
ACE_1/Admin(config-cmap-http-lb)# match protocol http url /MeetMeIVR/.*
ACE_1/Admin(config-cmap-http-lb)# exit
```

Configuring Layer 7 SIP Class Maps

To a create Layer 7 SIP class map for load balancing, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)# class-map type sip loadbalance match-any` *map_name*	Creates a Layer 7 class map for load balancing SIP traffic. The match-any keyword indicates that a message matches this class map if any of the configured match statements are true.
Step 2	`ACE_1/Admin(config-cmap-sip-lb)# match source-address` *ip_address* [*mask*]	Specifies the source IP address (with optional mask) to match for this class map.
Step 3	`ACE_1/Admin(config-cmap-sip-lb)# match sip header` *header_name* `header-value` *expression*	Configures a value (or set of values) in the specified SIP header to match for this class map. Expression uses regular expression syntax.
Step 4	`ACE_1/Admin(config-cmap-sip-lb)# exit`	Exits SIP class map load balancing configuration mode.

The following example shows how to configure a SIP load-balancing class map to match traffic with any value of Call-ID:

```
ACE_1/Admin(config)# class-map type sip loadbalance match-any SIP-L7
ACE_1/Admin(config-cmap-sip-lb)# match sip header Call-ID header-value ".*"
```

Configuring Layer 3 and Layer 4 Class Maps

To create a Layer 3 and Layer 4 class map, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)# class-map match-any` *map_name*	Creates a Layer 3 and Layer 4 class map.
Step 2	`ACE_1/Admin(config-cmap)# match virtual-address` *vip_address* { **tcp** | **udp** } **eq** *port_number*	Configures the ACE virtual IP address, protocol, and port number to match for this class map.
Step 3	`ACE_1/Admin(config-cmap)# match port` { **tcp** | **udp** } **eq sip**	Configures the TCP or UDP port number to match for this class map. SIP has the value 5060.

The following example shows how to create a Layer 3 and 4 class map that matches the IVR traffic arriving at the virtual IP address:

```
ACE_1/Admin(config)# class-map match-any IVR-VIP
ACE_1/Admin(config-cmap)# match virtual-address 10.22.139.103 tcp eq 8080
```

The following example shows how to create a Layer 3 and 4 class map for all SIP UDP traffic:

```
ACE_1/Admin(config)# class-map match-any SIP_UDP_CLASS
ACE_1/Admin(config-cmap)# match port udp eq sip
ACE_1/Admin(config-cmap)# exit
```

The following example creates a Layer 3 and 4 class map for all SIP traffic:

```
ACE_1/Admin(config)# class-map match-any SIP_TRAFFIC
ACE_1/Admin(config-cmap)# match port udp eq sip
ACE_1/Admin(config-cmap)# match port tcp eq sip
ACE_1/Admin(config-cmap)# exit
```

The following example shows how to create a Layer 3 and 4 class map to match all SIP traffic (UDP and TCP) arriving at the specified virtual IP address:

```
ACE_1/Admin(config-if)# class-map match-any SIP_VIP_CLASS
ACE_1/Admin(config-cmap-mgmt)# match virtual-address 10.22.139.103 udp eq sip
ACE_1/Admin(config-cmap-mgmt)# match virtual-address 10.22.139.103 tcp eq sip
```

Configuring Management Class Maps

To allow remote network traffic to pass through the ACE, you must create a management traffic policy, which requires a management class map.

To configure a management class map, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)# class-map type management match-any` *map_name*	Creates a Layer 3 and Layer 4 class map for management traffic. The match-any keyword indicates that a message matches this class map when any of the configured match statements are true.
Step 2	`ACE_1/Admin(config-cmap-mgmt)# match protocol` *protocol_name* [**any** | **source_address** *ip_address mask*]	Configures a management protocol to match for this class map. You can configure the match statement to match any source address or configure a specific source IP address and mask.
Step 3	`ACE_1/Admin(config-cmap-mgmt) exit`	Exits class map HTTP load balancing configuration mode.

The following example shows how to create a management-type class map that matches traffic from any source that matches any of the specified protocols:

```
ACE_1/Admin(config-if)# class-map type management match-any REMOTE_ACCESS
ACE_1/Admin(config-cmap-mgmt)# match protocol xml-https any
ACE_1/Admin(config-cmap-mgmt)# match protocol icmp any
ACE_1/Admin(config-cmap-mgmt)# match protocol telnet any
ACE_1/Admin(config-cmap-mgmt)# match protocol ssh any
ACE_1/Admin(config-cmap-mgmt)# match protocol http any
ACE_1/Admin(config-cmap-mgmt)# match protocol https any
ACE_1/Admin(config-cmap-mgmt)# match protocol snmp any
ACE_1/Admin(config-cmap-mgmt)# exit
```

Configuring Policy Maps

A policy map defines a series of actions that you want to apply to traffic that matches one or more of the associated class maps.

This section addresses policy map configuration and includes the following topics:

- Configuring Layer 4 Policy Maps, page 15-18

Configuring Management Policy Maps

A management policy map specifies policy for network management traffic that is received by the ACE.

To create a management policy map, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)#` **`policy-map type management first-match | match-any`** *`map_name`*	Creates a policy map for management traffic.
Step 2	`ACE_1/Admin(config-pmap-mgmt)#` **`class`** *`name1`*	Associates a class map with this policy map. You can associate multiple class maps with a policy map.
Step 3	`ACE_1/Admin(config-pmap-mgmt-c)#` **`permit | deny`**	Specifies whether to permit or deny the traffic that matches the class map.
Step 4	`ACE_1/Admin(config-pmap-mgmt-c)` **`exit`**	Exits management policy map configuration mode.

The following example shows how to create a policy map to allow remote management access to the Cisco TelePresence Exchange System:

```
ACE_1/Admin(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
ACE_1/Admin(config-pmap-mgmt)# class REMOTE_ACCESS
ACE_1/Admin(config-pmap-mgmt-c)# permit
```

Configuring Layer 7 Load Balancing Policy Maps

A Layer 7 load balancing policy map specifies the traffic (based on a class map) to send to each server farm for load balancing. The order of classes in the policy map is significant, as traffic is sent to the server farm that is associated with the first matching traffic class in the policy.

To create a Layer 7 load balancing policy map, do the following task:

	Command	Purpose
Step 1	`ACE_1/Admin(config)#` **`policy-map type loadbalance first-match | match-any`** *`map_name`*	Creates a Layer 7 load-balancing policy map for HTTP traffic.
Step 2	`ACE_1/Admin(config-pmap-lb)#` **`class`** *`name1`*	Associates a class map with this policy map. You can associate multiple class maps with a policy map.
Step 3	`ACE_1/Admin(config-pmap-lb-c)#` **`sticky-serverfarm`** *`name`*	Specifies that the traffic that matches this class is load-balanced to the specified sticky server farm.
Step 4	`ACE_1/Admin(config-pmap-lb-c)` **`exit`**	Exits class map HTTP load balancing configuration mode.

The following example shows how to create a Layer 7 policy map to load balance IVR traffic by using the IVR_STICKY server farm. The system load balances all other traffic by using the WEB_STICKY server farm:

```
ACE_1/Admin(config)# policy-map type loadbalance first-match VXML-LB
ACE_1/Admin(config-pmap-lb)# class IVR
ACE_1/Admin(config-pmap-lb-c)# sticky-serverfarm IVR_STICKY
ACE_1/Admin(config-pmap-lb-c)# class class-default
ACE_1/Admin(config-pmap-lb-c)# sticky-serverfarm WEB-STICKY
```

Note Class-default is a pre-configured class map that matches all traffic.

The following example shows how to create a policy map to load balance SIP traffic across the SIP_FARM server farm:

```
ACE_1/Admin(config)# policy-map type loadbalance sip first-match L7-POLICY
ACE_1/Admin(config-pmap-lb)# class SIP-L7
ACE_1/Admin(config-pmap-lb-c)# sticky-serverfarm SIP_FARM
```

Configuring Layer 4 Policy Maps

To create a Layer 4 policy map, do the following task:

	Command	Purpose
Step 1	ACE_1/Admin(config)# **policy-map multi-match** *map_name*	Creates a Layer 4 load balancing policy map. Multi-match allows the inclusion of multiple network traffic-related actions in the same policy map.
Step 2	ACE_1/Admin(config-pmap)# **class** *name1*	Associates a class map with this policy map.
Step 3	ACE_1/Admin(config-pmap-c)# **loadbalance vip inservice**	Enables the VIP for server load-balancing.
Step 4	ACE_1/Admin(config-pmap-c) **loadbalance policy** *name*	Specifies a Layer 7 load-balancing policy map to associate with this Layer 4 policy map.
Step 5	ACE_1/Admin(config-pmap-c)# **appl-parameter sip advanced-options syslog**	Associates a SIP parameter map with this policy.
Step 6	ACE_1/Admin(config-pmap-c)# **loadbalance vip icmp-reply**	Enables the VIP to respond to ICMP ECHO requests.
Step 7	ACE_1/Admin(config-pmap-c)# **connection advanced-options**	Associates a connection parameter map with this policy.
Step 8	ACE_1/Admin(config-pmap-c)# **inspect sip**	Enables packet inspection of the SIP packets.
Step 9	ACE_1/Admin(config-pmap-c) **exit**	Exits policy map configuration mode.

The following example shows how to create a Layer 4 policy map for incoming HTTP traffic on a VIP (specified in the class) and apply a Layer 7 load balancing policy:

```
ACE_1/Admin(config)# policy-map multi-match IVR_LB
ACE_1/Admin(config-pmap)# class IVR-VIP
ACE_1/Admin(config-pmap-c)# loadbalance vip inservice
ACE_1/Admin(config-pmap-c)# loadbalance policy VXML-LB
ACE_1/Admin(config-pmap-c)# loadbalance vip icmp-reply active
```

The following example shows how to create a Layer 4 policy map for incoming SIP traffic on a VIP (specified in the class) and apply a Layer 7 load balancing policy:

```
ACE_1/Admin(config)# policy-map multi-match L4-POLICY
ACE_1/Admin(config-pmap)# class SIP_VIP_CLASS
ACE_1/Admin(config-pmap-c)# loadbalance vip inservice
ACE_1/Admin(config-pmap-c)# loadbalance policy L7-POLICY
ACE_1/Admin(config-pmap-c)# loadbalance vip icmp-reply active
ACE_1/Admin(config-pmap-c)# appl-parameter sip advanced-options syslog
ACE_1/Admin(config-pmap-c)# inspect sip
```

The following example shows how to create a Layer 4 policy map to enable traffic inspection for all SIP traffic:

```
ACE_1/Admin(config)# policy-map multi-match SIP_INSPECT
ACE_1/Admin(config-pmap)# class SIP_TRAFFIC
ACE_1/Admin(config-pmap-c)# inspect sip
```

The following example shows how to apply UDP connection timeout settings for all SIP UDP traffic:

```
ACE_1/Admin(config)# policy-map multi-match UDP_TIMEOUT
ACE_1/Admin(config-pmap)# class SIP_UDP_CLASS
ACE_1/Admin(config-pmap-c)# connection advanced-options UDP-Timeout
```

Configuring VLAN Interfaces

Each Gigabit Ethernet port must be associated with a VLAN. For redundant configurations of the Cisco TelePresence Exchange System using the ACE, you must also define a fault-tolerant (FT) VLAN. The redundant ACE pair constantly communicate over the dedicated FT VLAN to determine the operating status of each appliance. The standby member uses the heartbeat packet to monitor the health of the active member. The active member uses the heartbeat packet to monitor the health of the standby member. Each ACE peer can also contain one or more FT groups. Each FT group consists of two members: one active context and one standby context. An FT group has a unique group ID that you assign.

You also must configure a different IP address within the same subnet on each appliance for the FT VLAN.

Note Do not use this dedicated VLAN for any other network traffic, including HSRP and data.

For multiple contexts, the FT VLAN resides in the system configuration file. Each FT VLAN on the ACE has one unique MAC address that is associated with it. The ACE uses these device MAC addresses as the source or destination MACs for sending or receiving redundancy protocol state and configuration replication packets.

Note An ACE appliance and an ACE module operating as peers cannot operate as redundant pairs for the Cisco TelePresence Exchange System. System redundancy must employ the same ACE device type and software release.

To configure a VLAN interface, do the following task:

	Command	Purpose
Step 1	ACE_1/Admin(config)# **interface vlan** *vlan_number*	Enters configuration mode for the specified VLAN interface.
Step 2	ACE_1/Admin(config-if)# **ip address** *ip-address mask*	Configures the IP address and mask for the VLAN interface.
Step 3	ACE_1/Admin(config-if)# **alias ip address** *ip-address mask*	Defines the default route when a redundant ACE configuration exists. (Required only for redundant ACE configurations).
Step 4	ACE_1/Admin(config-if)# **peer ip address** *ip-address mask*	Defines the IP address and mask for the fault tolerant VLAN interface. (Required only for redundant ACE configurations).
Step 5	ACE_1/Admin(config-if)# **normalization send-reset**	Enables sending a RST to the peer so it can reset its TCP connections for any non-SYN packets that are a connection miss.
Step 6	ACE_1/Admin(config-if)# **access-group** {**input** | **output**} *name*	Associates the specified access group list (ACL) with the VLAN. The ACL will be applied to all incoming traffic (input) or outgoing traffic (output).
Step 7	ACE_1/Admin(config)# **service-policy** { **input** | **output** } *name*	Associates the specified service policy with the VLAN. The service policy will be applied to all incoming traffic (input) or outgoing traffic (output). (Not configured on fault tolerant VLANs).
Step 8	ACE_1/Admin(config)# **ft interface** *interface_name*	Creates a fault tolerant VLAN to provide a communication path for updates from the active ACE to its peer (standby). (Required only for redundant ACE configurations).
Step 9	ACE_1/Admin(config-ft-intf)# **ip address** *ip-address mask*	Configures the IP address and mask for the VLAN interface. (Required only for redundant ACE configurations).
Step 10	ACE_1/Admin(config-ft-intf)# **peer ip address** *ip-address mask*	Specifies the IP address and mask of the ACE peer. (Required only for redundant ACE configurations).
Step 11	ACE_1/Admin(config-ft-intf)# **no shutdown**	Enables the VLAN interface.
Step 12	ACE_1/Admin(config-ft-intf)# **exit**	Exits fault tolerant interface configuration mode.
Step 13	ACE_1/Admin(config)# **ft peer** *peer_id*	Configures an ACE local redundancy peer.
Step 14	ACE_1/Admin(config-ft-peer)# **ft-interface vlan** *vlan_id*	Associates the fault-tolerant (FT) VLAN with the peer. **Note** This VLAN ID must also be configured on the switch. Only a layer 2 definition is required.
Step 15	ACE_1/Admin(config-ft-peer)# **heartbeat interval** frequency **heartbeat count** number	Configures the heartbeat interval and count for the fault-tolerant peer. Values are in milliseconds (ms).
Step 16	ACE_1/Admin(config-ft-peer)# **query-interface vlan** vlan_id	Defines the actual (routable) VLAN and interface that the fault-tolerant peer uses to send health-check and replication messages. A query interface allows the standby ACE to determine whether the active ACE is down or if there is a connectivity problem with the FT VLAN. A query interface helps prevent two redundant contexts from becoming active at the same time for the same FT group.

	Command	Purpose
Step 17	`ACE_1/Admin(config-ft-peer)# no shutdown`	Enables the query interface.
Step 18	`ACE_1/Admin(config-ft-peer)# exit`	Exits fault-tolerant peer configuration mode.
Step 19	`ACE_1/Admin(config)# ft group` *group_id*	Creates a fault-tolerant group for redundancy.
Step 20	`ACE_1/Admin(config-ft-group)# peer` *peer_id*	Associates the peer with the fault-tolerant group.
Step 21	`ACE_1/Admin(config-ft-group)# no preempt`	Disables preemption on the fault-tolerant group. Preemption ensures that the group member with the higher priority always asserts itself and becomes the active member.
Step 22	`ACE_1/Admin(config-ft-group)# priority` *number*	Configures the priority of the active group member. Values are 1 to 255. Configure a higher priority for the group on the module on which you want the active member to initially reside.
Step 23	`ACE_1/Admin(config-ft-group)# associate-context` name	Associates a context with each fault-tolerant group. You must associate the local ACE with the fault-tolerant group. You can assign multiple contexts.
Step 24	`ACE_1/Admin(config-ft-group)# inservice`	Places a fault-tolerant group in service.

Non-Redundant Configuration

The following example shows how to configure VLAN 340 as the outside interface. The **service-policy** commands activate the Layer 3 and Layer 4 policies on this VLAN. The Layer 7 load-balancing policies become active because they are encapsulated in the Layer 3 and Layer 4 policies:

```
ACE_1/Admin(config)# interface vlan 340
ACE_1/Admin(config-if)# description OUTSIDE network
ACE_1/Admin(config-if)# ip address 10.22.139.102 255.255.255.240
ACE_1/Admin(config-if)# normalization send-reset
ACE_1/Admin(config-if)# access-group input ALL
ACE_1/Admin(config-if)# service-policy input remote_mgmt_allow_policy
ACE_1/Admin(config-if)# service-policy input L4-POLICY
ACE_1/Admin(config-if)# service-policy input UDP_TIMEOUT
ACE_1/Admin(config-if)# service-policy input IVR_LB
ACE_1/Admin(config-if)# no shutdown
ACE_1/Admin(config-if)# exit
```

The following example shows how to configure the VLAN 350 interface as the inside interface:

```
ACE_1/Admin(config)# interface vlan 350
ACE_1/Admin(config-if)# description INSIDE network
ACE_1/Admin(config-if)# ip address 10.22.139.113 255.255.255.240
ACE_1/Admin(config-if)# normalization send-reset
ACE_1/Admin(config-if)# access-group input ALL
ACE_1/Admin(config-if)# service-policy input remote_mgmt_allow_policy
ACE_1/Admin(config-if)# service-policy input UDP_TIMEOUT
ACE_1/Admin(config-if)# service-policy input SIP_INSPECT
ACE_1/Admin(config-if)# no shutdown
ACE_1/Admin(config-if)# exit
```

Redundant Configuration

The following example shows how to configure VLAN 340 as the outside interface to support redundancy. The **service-policy** commands activate the Layer 3 and Layer 4 policies on this VLAN. The Layer 7 load-balancing policies become activated because they are encapsulated in the Layer 3 and Layer 4 policies:

```
ACE_1/Admin(config)# interface vlan 340
ACE_1/Admin(config-if)# description OUTSIDE network
ACE_1/Admin(config-if)# ip address 10.22.139.102 255.255.255.240
ACE_1/Admin(config-if)# alias 10.22.139.108 255.255.255.240
ACE_1/Admin(config-if)# peer ip address 10.22.139.104 255.255.255.240
ACE_1/Admin(config-if)# normalization send-reset
ACE_1/Admin(config-if)# access-group input ALL
ACE_1/Admin(config-if)# service-policy input remote_mgmt_allow_policy
ACE_1/Admin(config-if)# service-policy input UDP_TIMEOUT
ACE_1/Admin(config-if)# service-policy input L4-POLICY
ACE_1/Admin(config-if)# service-policy input IVR_LB
ACE_1/Admin(config-if)# no shutdown
ACE_1/Admin(config-if)# exit
```

The following example shows how to configure the VLAN 350 interface as the inside interface:

```
ACE_1/Admin(config)# interface vlan 350
ACE_1/Admin(config-if)# description INSIDE network
ACE_1/Admin(config-if)# ip address 10.22.139.114 255.255.255.240
ACE_1/Admin(config-if)# alias 10.22.139.113 255.255.255.240
ACE_1/Admin(config-if)# peer ip address 10.22.139.117 255.255.255.240
ACE_1/Admin(config-if)# no icmp-guard
ACE_1/Admin(config-if)# normalization send-reset
ACE_1/Admin(config-if)# access-group input ALL
ACE_1/Admin(config-if)# service-policy input remote_mgmt_allow_policy
ACE_1/Admin(config-if)# service-policy input UDP_TIMEOUT
ACE_1/Admin(config-if)# no shutdown
ACE_1/Admin(config-if)# exit
```

The following example shows how to configure the fault tolerant VLAN 999 interface on the trunk outside interface:

Note The fault-tolerant VLAN does not need to be routable; however, you must define the fault-tolerant VLAN on the switch that connects to the ACE to ensure layer 2 connectivity.

```
ACE_1/Admin(config)# ft interface vlan 999
ACE_1/Admin(config-ft-intf)# ip address 10.1.1.1 255.255.255.0
ACE_1/Admin(config-ft-intf)# peer ip address 10.1.1.2 255.255.255.0
ACE_1/Admin(config-ft-intf)# no shutdown
ACE_1/Admin(config-ft-intf)# exit
ACE_1/Admin(config)# ft peer 1
ACE_1/Admin(config-ft-peer)# heartbeat interval 200
ACE_1/Admin(config-ft-peer)# heartbeat count 10
ACE_1/Admin(config-if)# ft-interface vlan 999
ACE_1/Admin(config-if)# query-interface vlan 340
ACE_1/Admin(config)# ft group 1
ACE_1/Admin(config-ft-group)# peer 1
ACE_1/Admin(config-ft-group)# no preempt
ACE_1/Admin(config-ft-group)# priority 110
ACE_1/Admin(config-ft-group)# associate-context Admin
ACE_1/Admin(config-ft-group)# inservice
```

Configuring Miscellaneous Parameters

This section describes additional ACE configurations for the Cisco TelePresence Exchange System and includes the following topics:

Configuring the IP Default Route

Configure the default IP route for the inside VLAN to be the ACE inside interface. This configuration ensures that all traffic originating from the Cisco TelePresence Exchange System cluster transits through the ACE.

To define the default IP route (gateway), enter the following command:

```
ACE_1/Admin(config)# ip route 0.0.0.0 0.0.0.0 10.22.139.97
```

Configuring UDP Connection Timeout

Create a connection parameter map to define the UDP inactivity timeout value:

```
parameter-map type connection name
set timeout inactivity seconds
```

The following example shows how to create a parameter map with a timeout value of one second:

```
ACE_1/Admin(config)# parameter-map type connection UDP-timeout
ACE_1/Admin(config-parammap-conn)# set timeout inactivity 1
```

Enabling SysLog SIP Messages

Use the **parameter-map** command to set the logging value for SIP syslogs.

The following example shows how to create a parameter map to enable logging for SIP traffic:

```
ACE_1/Admin(config)# parameter-map type sip syslog
ACE_1/Admin(config-parammap-conn)# logging all
```

Configuring the Sticky Resource Class

Sticky groups require system resources to store information about active sessions.

Create a sticky resource class to reserve the required system resources.

You define the resource requirement as a percentage of the total available resources.

For example, you can create a sticky resource class that allows access to the ACE for no less that 20 percent of the total number of stickiness connections that the ACE appliance supports. You must configure a minimum value for sticky to allocate resources for sticky entries, because the sticky software receives no resources under the unlimited (no limit) setting. The maximum value is either the same as the minimum value (equal-to-min) or has no limit.

To configure a sticky resource class and the number of sticky entries supported, do the following task:

Step 1 To define a resource class that allows call stickiness, enter the following command:

```
ACE_1/Admin#(config)# resource-class sticky
ACE_1/Admin#(config-resource)#
```

Step 2 To define the minimum and maximum entries allowed in the sticky resource class table, enter the following commands:

```
ACE_1/Admin#(config-resource)# limit-resource all minimum 0.00 maximum unlimited
ACE_1/Admin#(config-resource)# limit-resource sticky minimum 20.00 maximum
equal-to-min
```

Assigning the Admin Context to the Sticky Resource Class

You can operate the ACE in a single context or in multiple contexts. Multiple contexts use virtualization to partition the ACE into multiple virtual devices. Each context can contain its own set of policies, interfaces, resources, and administrators.

By default, the system enables a single virtual context known as the Admin context.

Use the **member** command to associate the sticky resource class to the Admin context.

The following example shows how to assign the sticky resource class to the default Admin context:

```
ACE_1/Admin(config)# context Admin
ACE_1/Admin(config-context)# member sticky
```

Configuring ACE Logging Options

You can configure the logging severity level, which specifies the severity system messages that the ACE logs. The ACE supports eight logging levels. Severity level values are 0 to 7; the lower the level number, the more severe the error.

The ACE logs messages of the specified level and those lower. For example, if the logging severity level is 3, the ACE logs messages with a severity level of 0, 1, 2, and 3.

Table 15-1 lists the log message severity levels.

Table 15-1 Log Message Severity Levels

Level Number	Level Keyword	Description
0	emergency	System unusable. For example, the ACE has shut down and cannot restart, or the system has experienced a hardware failure.
1	alert	Immediate action needed. For example, one of the ACE subsystems is not running.
2	critical	Critical condition. For example, the ACE has encountered a critical condition that requires immediate attention.

Table 15-1 Log Message Severity Levels (continued)

Level Number	Level Keyword	Description
3	error	Error condition. For example, error messages are conveyed about software or hardware malfunctions.
4	warning	Warning condition. For example, the ACE encountered an error condition that requires attention but is not interfering with the operation of the device.
5	notification	Normal but significant condition. For example, interface up/down transitions and system restart messages are conveyed.
6	informational	Informational message only. For example, reload requests and low-process stack messages are conveyed.
7	debugging	Appears during debugging only.

For more details on ACE SysLog Messages, see the *Cisco ACE 4700 Series Appliance System Message Guide*, at http://www.cisco.com/en/US/products/ps7027/products_installation_and_configuration_guides_list.html.

To enable logging of syslog messages on the ACE, do the following task:

Step 1 To enable logging to all output locations, enter the following commands:

```
ACE_1/Admin# configure
ACE_1/Admin#(config)# logging enable
```

To stop message logging to all output locations, enter the **no logging enable** command at the configuration mode.

Step 2 To enable logging of syslog messages and to assign a security level to specify which syslog messages the system logs, do this task:

a. To enable logging of syslog messages during a console session by using the **logging console** *severity_level* configuration mode command, enter the following command:

```
ACE_1/Admin#(config)# logging console 2
```

By default, the ACE does not display syslog messages during console sessions. To disable logging on the ACE, enter the **no logging console** command at the configuration mode.

b. To identify the date and time of a syslog message by using the **logging timestamp** configuration mode command, enter the following command:

```
ACE_1/Admin#(config)# logging timestamp
```

By default, the ACE does not generate a timestamp for syslog messages.

c. To identify the severity level of messages that are sent to the syslog server by using the **logging trap** *severity_level* configuration mode command, enter the following command:

```
ACE_1/Admin#(config)# logging trap 3
```

To disable logging of traps, enter the **no logging trap** command at the configuration mode.

d. To enable logging of Simple Network Management Protocol (SNMP) messages and to set the severity level for log messages that are sent to a network management system (NMS) by using the **logging history** *severity_level* configuration mode command, enter the following command:

```
ACE_1/Admin#(config)# logging history 7
```

To disable logging of SNMP messages, enter the **no logging history** command at the configuration mode.

e. To enable system logging to a local buffer and to limit the messages sent to the buffer based on severity level by using the **logging buffered** *severity_level* configuration mode command, enter the following command:

```
ACE_1/Admin#(config)# logging buffered 7
```

f. To change the logging facility to a value other than the default of 20 (LOCAL4) by using the **logging facility** *number* configuration mode command, enter the following command:

```
ACE_1/Admin#(config)# logging facility 23
```

The number can be a value from 16 (LOCAL0) to 23 (LOCAL7).

Most UNIX systems expect messages to use facility 20. The ACE allows you to change the syslog facility type to identify the behavior of the syslog daemon (syslogd) on the host.

To reset the logging facility to the default value of 20, enter the **no logging facility** command at the configuration mode.

g. To specify that the ACE hostname serves as the device ID within the syslog message, enter the following command:

```
ACE_1/Admin#(config)# logging device-id hostname
```

To disable use of the hostname as the device ID in the syslog message, enter the **no logging device-id** command.

h. To specify the syslog server (host) that receives the ACE syslog messages, enter the following command:

```
ACE_1/Admin#(config)# logging host ip_address
```

For the ip_address variable, enter the IP address of the host that serves as the syslog server.

You do not need to specify a port for the syslog server because by default it uses a UDP port of 514.

You can use multiple logging host commands to specify additional servers to receive the syslog messages.

To disable logging of ACE syslog messages to a syslog server, enter the **no logging host** *ip_address.*

i. To control the display of a specific system logging message or to change the severity level that is associated with the specified system logging message by using the **logging message syslog_id** [***level*** *severity_level]* configuration mode command, enter the following commands:

```
ACE_1/Admin#(config)# logging message 111088 level 3
ACE_1/Admin#(config)# logging message 607002 level 3
ACE_1/Admin#(config)# logging message 607004 level 3
ACE_1/Admin#(config)# logging message 607005 level 3
```

To disable logging of the specified syslog message, use the **no logging message** *syslog_id* command at the configuration mode.

CHAPTER 16

Configuring the Cisco TelePresence Multipoint Switch

Revised July 3, 2012

The following sections describe how to configure the Cisco TelePresence Multipoint Switch:

Additional information about Cisco TelePresence Multipoint Switch configuration is available at http://www.cisco.com/en/US/docs/telepresence/multipoint_switch/1_8/administration/guide/config.html.

Configuring System Settings

You configure system settings for the Cisco TelePresence Multipoint Switch Administration during software setup. The following sections describe how to make changes to the system settings:

Configuring IP Settings

Procedure

To configure the IP settings, do the following procedure:

Step 1 From the left navigation pane, choose **Configure > System Settings**.

Step 2 Click the **IP** tab.

A table with IP Settings configuration fields is displayed. Table 16-1 describes the fields.

Step 3 Configure the required IP Setting fields, and then do one of the following:

- To register new or modified settings, click **Apply**.
- To restore the original settings, click **Cancel**.

Table 16-1 IP Settings

Field or Button	Setting
MAC Address	View only. MAC address of the Cisco 7800 Series Media Convergence Server (MCS) on which the Cisco TelePresence Multipoint Switch is located.
Hostname	View only. Hostname configured for the MCS server on which the Cisco TelePresence Multipoint Switch is located.
Domain Name	Domain name for the MCS server on which the Cisco TelePresence Multipoint Switch is located.
Primary DNS	IP address of the primary Domain Name System (DNS) server for the MCS server on which the Cisco TelePresence Multipoint Switch is located.
Secondary DNS	IP address of the secondary Domain Name System (DNS) server for the MCS server on which the Cisco TelePresence Multipoint Switch is located.
Ethernet Card	View only. Ethernet card on the MCU server that connects to the network.
IP Address	IP address of the Cisco TelePresence Multipoint Switch. **Note** After changing the IP address, close your browser window, and then log in to the Cisco TelePresence Multipoint Switch again using your new IP address.
Subnet Mask	Subnet mask associated with the IP Address.
Default Gateway	Default gateway IP address for the Cisco TelePresence Multipoint Switch.

Editing Route Pattern Settings

Route pattern settings define route patterns (strings of digits that can direct calls for specific systems) and access numbers that are associated with the Cisco TelePresence Multipoint Switch.

Procedure

To edit the route pattern settings, do the following procedure:

Step 1 From the left navigation pane, choose **Configure > System Settings**.

Step 2 Click the **Route Pattern** tab.

The Route Pattern window is displayed. Table 16-2 describes the fields.

Step 3 Modify the route pattern settings as required, and then do one of the following:

- To register new or modified settings, click **Apply**.
- To restore the original settings, click **Cancel**.

Table 16-2 Route Pattern Settings

Field or Button	Setting
Route Pattern Start	Defines the first number in your route pattern. Use this number in the Vendor Config—Min Static Meeting ID field when you configure the CTMS resource for this server in the Cisco TelePresence Exchange System.
Route Pattern End	Defines the last number in your route pattern. Use this number in the Vendor Config—Max Static Meeting ID field when you configure the CTMS resource for this server in the Cisco TelePresence Exchange System.
Access Number	Displays the first number in the route pattern. The Cisco TelePresence Multipoint Switch (CTMS) automatically chooses the first number in the range. The access number serves as the dial-in number for all scheduled meetings. This number also acts as the caller ID when the CTMS dials out for meetings.
Access Name	Descriptive name for the access number. The maximum number of characters is 20. Use this Access Name when provisioning this CTMS in Cisco TelePresence Exchange System under **Media Resources > CTMS Resources**.

Configuring QoS Settings

Differentiated Services Code Point (DSCP) markings are used by the network to classify traffic priority, enabling a common queuing strategy throughout the network. Quality of Service (QoS) values define the DSCP traffic marking values that are used for network queuing for Cisco TelePresence Systems (CTS) and signaling.

Note Cisco recommends that the QoS settings for CTMS be consistent with the QoS settings for Unified CM and for Cisco TelePresence Systems endpoints, and that they align with your enterprise-wide queuing strategy.

Procedure

To configure QoS settings, do the following procedure:

Step 1 From the left navigation pane, choose **Configure > System Settings**.

Step 2 Click the **QoS** tab.

A table with QoS Settings configuration fields is displayed.

Step 3 Choose from the drop-down list or enter the following values for the QoS settings:

- DSCP for CTS Media—**CS5(precedence 5) DSCP (101000)**
- DSCP for CUCV Media—**AF41 DSCP (100010)**
- DSCP for Signaling—**CS5(precedence 5) DSCP (101000)**

Step 4 After choosing the QoS settings, do one of the following:

- To register new or modified settings, click **Apply**.
- To restore the original settings, click **Cancel**.

Configuring Resource Management

Procedure

To configure or edit Resource Management settings, do the following procedure:

Step 1 From the left navigation pane, choose **Configure > System Settings**.

Step 2 Click the **Resources** tab.

A table with the Resources configuration fields is displayed. Table 16-3 describes the fields.

Step 3 For the Maximum Segments setting, enter a value of **48**.

Step 4 For the Adhoc Segments setting, enter a value of **48**.

Step 5 After entering the settings, do one of the following:

- To register new or modified settings, click **Apply.**
- To restore the original settings, click **Cancel.**

Table 16-3 Resource Management Settings

Field or Button	Setting
Maximum Segments	Defines the total number of table segments (individual video displays) that the Cisco TelePresence Multipoint Switch supports. Enter a value of 48.

Table 16-3 Resource Management Settings (continued)

Field or Button	Setting
Adhoc Segments	Defines the maximum number of table segments that are available for impromptu meetings. Enter a value of 48.
Schedulable Segments	View only. Displays the number of table segments that are available at any one time for scheduled meetings. Cisco TelePresence Multipoint Switch automatically derives this value by subtracting the defined number of Ad Hoc Table Segments from the defined number of Maximum Table Segments.

About SNMP Settings

You configure all SNMP settings through the Cisco TelePresence Multipoint Switch command line interface.

SNMP monitors the system status (choose Monitoring > System Status for system status details). You can designate a particular server on which the system gathers and stores SNMP trap messages. Configuration requires username and password authentication.

By default, the system enables the SNMP service and the following SNMP settings:

- SNMPv3 username set to **mrtg**.
- SNMPv2c username set to **public**. This name is for internal use of the system and should not be deleted.

Caution Do not delete the SNMPv2c and SNMPv3 usernames that are set by the system.

Note By default, the system does not configure a trap receiver. Use CLI commands to configure SNMP trap receiver information.

For additional information about configuring SNMP on the Cisco TelePresence Multipoint Switch, see the *Cisco TelePresence Multipoint Switch Release 1.8 Administration Guide*, at http://www.cisco.com/en/US/docs/telepresence/multipoint_switch/1_8/administration/guide/CTMS_Release1_8.html.

The Cisco TelePresence Multipoint Switch MIBs are listed at ftp://ftp-sj.cisco.com/pub/mibs/supportlists/ctms/ctms-supportlist.html.

Configuring Unified CM Settings

The following sections describe how to make changes to the Cisco Unified Communications Manager (Unified CM) settings by using the Cisco TelePresence Multipoint Switch administration user interface:

- Configuring Unified CM Settings on the Cisco TelePresence Multipoint Switch, page 16-6
- Configuring SIP Profile Settings, page 16-6

Configuring Unified CM Settings on the Cisco TelePresence Multipoint Switch

In order for the Cisco TelePresence Multipoint Switch to interoperate with the Cisco TelePresence Exchange System, you must configure a Unified CM entry in CTMS for the virtual IP address of the Cisco Application Control Engine, and an entry for each of the Cisco TelePresence Exchange System call engine servers.

Procedure

To configure Unified CM settings, do the following procedure:

Step 1 From the left navigation pane, choose **Configure > Unified CM**.

Step 2 Click the **Unified CM** tab.

A table with the Unified CM configuration fields is displayed. Table 16-4 describes the fields.

Step 3 Configure the Unified CM settings, and then do one of the following:

- To register new or modified settings, click **Apply.**
- To restore the original settings, click **Cancel.**

Table 16-4 Unified CM Settings

Field or Button	Setting
Unified CM 1 through 5	Hostnames or IP address(es) of the Unified CM server. **Note** In the first field, enter the ACE virtual IP (VIP). Enter either the hostname or IP address of the two call engines of the Cisco TelePresence Exchange System in the second and third fields. Leave the fourth and fifth fields blank.
SIP Port	Use the default setting of 5060.

Configuring SIP Profile Settings

Procedure

To configure SIP Profile settings, do the following procedure:

Step 1 From the left navigation pane, choose **Configure > Unified CM**.

Step 2 Click the **SIP Profile Settings** tab.

Step 3 From the Transport Layer Protocol drop-down list, choose **TCP**.

Step 4 Do one of the following:

- To register new or modified settings, click **Apply**.
- To restore the original settings, click **Cancel**.

Configuring Meeting Parameters

The following topics describe the configurations necessary on the Cisco TelePresence Multipoint Switch to support Meet-Me meetings and static meetings:

Configuring the Meet-Me User and Password

To enable the two-minute warning functionality for Meet-Me meetings, you must create a specific Meet-Me user and password on the Cisco TelePresence Multipoint Switch.

Procedure

Step 1 In the left navigation pane, select **Configure > Access Management**.

Step 2 Click **New**.

Step 3 Enter the username and password for the Meet-Me user.

Step 4 Check the **Conference-Scheduler** check box.

Step 5 Click **Apply**.

Creating Static Meetings

You must create a minimum of 50 static meetings on the Cisco TelePresence Multipoint Switch to enable it to host Cisco TelePresence Exchange System meetings.

Static meetings are permanently available after you configure them. Each static meeting has its own associated meeting number, which the meeting attendees dial to attend the static meeting. You can also add participants to a static meeting through the Active Meetings page.

Static meetings must be contiguous values within a range of numbers such as 4085551000 through 4085551009. The range should be within the configured route pattern range. However, you cannot use the Route Pattern Start value as a static meeting value.

Note You must enter the same range of static meeting in the Vendor Config fields when you add a new CTMS resource to the Cisco TelePresence Exchange System by using the Administration Console. See the "Configuring CTMS Resources" section on page 9-6.

Before You Begin

Ensure that you have one contiguous range of access numbers that you can use for static meetings.

Procedure

To create a static meeting, do the following procedure:

Step 1 From the left navigation pane, choose **Manage > Static Meetings**.

The Static Meetings window displays all previously-configured static meetings.

Step 2 To add a static meeting entry, click **New**.

The Static Meetings entry window is displayed. Table 16-5 describes the fields.

Step 3 Enter values in the New Static Meetings window.

Step 4 To save new or modified settings, click **Apply**.

Step 5 Repeat Step 2 through Step 4 for each static meeting entry.

Static Meeting Fields

Table 16-5 Static Meeting Field Descriptions

Field or Button	Description
Access Number	Defines the phone number that participants call to attend this static meeting.
Meeting Description	Text describing or identifying this static meeting. The maximum number of characters for this field is 62 characters.
Switching Policy	Defines how Cisco TelePresence Multipoint Switch calls display during a meeting. Cisco TelePresence Multipoint Switch displays active speakers on screen. There are two active speaker display options; click the appropriate radio button to select: • **Speaker**—Each speaker is displayed on the screen as that speaker becomes the active speaker. • **Room**—All table segments for a particular room display on screen when any speaker in that room becomes the active speaker. If you are running CTS 1.3 or later, you can control how Cisco TelePresence calls display from the Cisco TelePresence phone interface. Press the **Speaker** softkey to display the active speaker; press the **Room** softkey to display all table segments from a particular room.
Maximum Rooms	Defines the maximum number of Cisco TelePresence rooms that can dial in to in a static multi-point meeting. The range for this setting is from 2 to 48.
Video Announce	When a new attendee joins the meeting, the new attendee appears on the screen for 2 seconds. Options are **Yes** and **No**.

Table 16-5 Static Meeting Field Descriptions (continued)

Field or Button	Description
Hosted Meeting	Identifies one room as the host for a meeting; other meeting rooms are not added to the meeting until the host room dials in. When you select **Video Announce** as an option, each meeting room is displayed in 2-second intervals in the order in which they join the meeting. Options are **Yes** and **No**. Click the appropriate radio button to select.
Host Room Number	Defines the host Cisco TelePresence System room number.
Interop	Determines whether the Cisco TelePresence Multipoint Switch handles interop meetings. Click the **No** radio button. Cisco TelePresence Server MSE 8710 and Cisco TelePresence MCU MSE 8510 manage interop meetings in the Cisco TelePresence Exchange Solution. Interop meetings include any standards-based H323 and ISDN endpoints.
Quality	This field sets the maximum default video quality for multipoint meetings: • Highest Detail, Best Motion: 1080p • Highest Detail, Better Motion: 1080p • Highest Detail, Good Motion: 1080p • High Detail, Best Motion: 720p • High Detail, Better Motion: 720p • High Detail, Good Motion: 720p The default is Highest Detail, Best Motion: 1080p
Meeting Security Policy	Click the appropriate radio button to select: **Secure—**Only secure Cisco TelePresence systems (and secure audio add-in attendees) can join this meeting; if non-secured Cisco TelePresence systems try to join, they are rejected. If a non-secure audio attendee joins the meeting (Conf/Join from the phone UI), that CTS will be dropped from the meeting. **Non-Secure—**Any Cisco TelePresence system can join the meeting. **Best-Effort—**The meeting is secure as long as all CTS and audio add-in attendees are secure. The meeting is downgraded to non-secured if a non-secured CTS or audio-add-in joins the meeting. **Note** Cisco recommends selecting **Best-Effort** and completing the procedures in the "Configuring Security Settings" section on page 16-10.
Maximum Presentation Bit Rate	Defines the maximum bit rate at which presentation video can be sent. Use the default setting of 30 FPS.

Configuring Security Settings

Cisco TelePresence Multipoint Switch provides support for secure communication between Cisco TelePresence devices by using Certificate Authority Proxy Function (CAPF). Each Cisco TelePresence product downloads a Locally Significant Certificate (LSC) from a CAPF server; communication between devices is then authenticated by using LSCs, Unified CM Root Certificates, and a CAPF Root Certificate.

To configure Cisco TelePresence Multipoint Switch for security, complete the following steps from the Unified CM administration window:

1. Activate and start the CAPF service.
2. Create application users.
3. Create Cisco Unified CM root certificates for every Unified CM server that is associated with the Cisco TelePresence Exchange System.
4. Create a CAPF root certificate.

After configuring security, complete the following steps from the Cisco TelePresence Multipoint Switch Security Settings window:

1. Upload the applicable Unified CM and CAPF root certificates.
2. Download the appropriate LSCs.

When all certificates are in place and the LSC is downloaded, the Cisco TelePresence Multipoint Switch reboots so that the security settings can take effect.

Security setting configuration is described in the following topics:

Configuring CAPF Profiles on Unified CM

Procedure

To configure CAPF profiles for the Cisco TelePresence Multipoint Switch, do the following procedure from the Unified CM administration software:

Step 1 Browse to https:// <*Unified CM-server-name*>:[8443]/ccmadmin/showHome.do.

For the Unified CM server, you can enter either its server name (if DNS is active) or its IP address. Optionally, you can also specify the port number (8443).

Step 2 From the Unified CM administration window, enter the username and password that you specified during Unified CM installation.

Step 3 Click **Login**.

Step 4 To create an application user in Unified CM, do the following:

a. In the administration window, from the **User Management** drop-down menu, choose **Application User**.

b. Click **Add New**.

The Application User Information window appears.

c. Enter data in all necessary fields.

Ensure that the user is included in the Standard CTI Enabled and Standard CTI Secure Connection groups. Under Permission Information, verify that the user also has the Standard AXL API Access and Standard CCM Admin Users roles.

d. To save your changes, click **Save**.

e. Repeat Step 4a to Step 4d to create an application user for each Cisco TelePresence Multipoint Switch in your network.

Step 5 To create an Application User CAPF profile in Unified CM, do the following:

a. In the administration window, from the **User Management** drop-down menu, choose **Application User CAPF Profile**.

b. Click **Add New**.

c. From the Application User drop-down list, choose the application user that you created in Step 4 and enter the appropriate CAPF profile fields for that user:

- Instance ID—Enter a unique identifier (alphanumeric) for each Cisco TelePresence Multipoint Switch.
- Certificate Operation—Choose **Install/Upgrade**.

Note Certificate Operation resets automatically to No Pending Operation after the system downloads a certificate. You must reset this field to Install/Upgrade for additional certificate downloads.

- Authentication Mode—Choose **By Authentication String** (default).
- Authentication String—Choose **Generate String** to create a randomly generated authentication string.

Note Make a note of the authentication string. You will use this information in the "Downloading LSC to Cisco TelePresence Multipoint Switch" section later in this chapter.

- Key size—Leave this field with the default value of **1024**.

d. To save your configuration, click **Save**.

e. To create an Application User CAPF Profile for each Cisco TelePresence Multipoint Switch in your network, click **Copy**, and then increment the Instance ID value by one for each Cisco TelePresence Multipoint Switch.

Downloading CAPF Root Certificates from Unified CM

Procedure

To download the CAPF root certificate from Unified CM, do the following procedure:

Step 1 In the **Cisco Unified OS Administration** in Cisco Unified CM, from the Security drop-down menu, choose **Certificate Management**.

Step 2 To display a list of certificates, click **Find**.

Step 3 Find the CAPF Root Certificate (for example, CAPF.der), and click the hypertext link for that certificate.

Step 4 To download the certificate, click **Download** and follow the download instructions.

Step 5 Save the CAPF Root Certificate to your desktop with the following name: **CAPF.der**.

Note The file name is case-sensitive.

Downloading Root Certificates from Unified CM

Procedure

To download Root certificates from Unified CM, do the following procedure:

Step 1 In the **Cisco Unified OS Administration** in Cisco Unified CM, from the Security drop-down menu, choose **Certificate Management**.

Step 2 To display a list of certificates, click **Find**.

Step 3 Find the Cisco Unified CM Root Certificate (for example, CallManager.der), and click the hypertext link for that certificate.

Step 4 To download the certificate, click **Download** and follow the download instructions.

Step 5 Save the Cisco Unified CM Root Certificate for the Publisher as **CUCM0.der**.

Note The file name is case-sensitive, and must be in the following format: CUCM#.der, where # is 0 for Publisher and 1 through 6 for Subscribers. If you have only one Cisco Unified CM server, download the certificate twice, and save the second copy as **CUCM1.der**.

Uploading CAPF and Unified CM Root Certificates

Procedure

To upload CAPF and root certificates to the Cisco TelePresence Multipoint Switch, do the following procedure from the Cisco TelePresence Multipoint Switch administration software:

Step 1 From the Cisco TelePresence Multipoint Switch administration window, choose **Configure > Security**.

Step 2 At the Security window, click **Install**.

Step 3 In the Certificate Upload panel that appears, do the following:

a. From the Unit drop-down list, choose **CAPF-Trust**.

b. From the Category drop-down list, choose **TRUST**.

c. Select the CAPF Root certificate that you downloaded from Cisco Unified CM (**CAPF.der**).

Note The file name is case-sensitive.

d. To upload the file onto the Cisco TelePresence Multipoint Switch, click **Install**.

Refresh the browser window to verify that the certificates have loaded.

Step 4 Upload the CUCM0.der file from your local machine by completing the following steps:

a. Return to the Security Settings window.

b. Click **Install**.

c. From the Unit drop-down list, choose **CTM-Trust**.

d. From the Category drop-down list, choose **TRUST**.

e. Select the Unified CM Root certificate that you downloaded from Cisco Unified CM (**CUCM0.der**).

Note The file name is case-sensitive.

f. To upload the file onto the Cisco TelePresence Multipoint Switch, click **Install**.

Refresh the browser window to verify that the certificates have loaded.

Step 5 Repeat Step 4 for the remaining CUCM#.der files.

Downloading LSC to Cisco TelePresence Multipoint Switch

Procedure

To download the LSC to the Cisco TelePresence Multipoint Switch, do the following procedure:

Step 1 From the Cisco TelePresence Multipoint Switch administration window, choose **Configure > Security**.

Step 2 At the Security window, click **Download LSC**.

Step 3 In the panel that appears, do the following:

a. In the CAPF Instance ID field, enter the CAPF instance ID that you created in Unified CM.

b. In the CAPF Auth String field, enter the CAPF Auth String that you generated in Unified CM.

c. In the TFTP Server Host field, enter the Unified CM TFTP server host.

d. In the TFTP Server Port field, enter **69**, which is the default value.

e. In the CAPF Server Host field, enter the Unified CM CAPF server host.

f. In the CAPF Server Port field, enter **3804**, which is the default value.

Step 4 To download LSC, click **Download LSC**.

Step 5 Click **OK** to confirm your choice. The LSCs are created.

After the LSC successfully downloads, the Cisco TelePresence Multipoint Switch reboots automatically.

Step 6 After the infrastructure device restarts, from the device administration interface, choose **Configure > Security**.

Verify that the Inter-Device Security field is set to secure, and that the Digital Security Certificate window displays the LSC certificates that were created, as listed in Table 16-1.

Table 16-6 LSC Certificate File Names

CTMS LSC Certificates	CTRS LSC Certificates	CTS-Man LSC Certificates
• CTMS_Cert_Chain.pem • CTMS.pem	• CTRS_Cert_Chain.pem • CTRS.pem	• CTM_Cert_Chain.pem • CTM.pem

Step 7 Obtain the SIP security trunk information by completing the following steps:

a. Click the radio button for the device .pem file.

b. Click the **View** button.

c. Note the information under Subject: in the file. You will use this information in the "Creating a SIP Trunk Security Profile" section that follows.

In the following example, you would note the subject name of **XXX-000**. (This is the X.509 Subject Name.)

```
Version: V3
  Subject: CN=XXX-000, O=cisco
  Signature Algorithm: SHA1withRSA, OID = 0.0.000.000000.0.0.0
```

Creating a SIP Trunk Security Profile

Procedure

To create a SIP trunk security profile, do the following procedure:

Step 1 Choose **System > Security Profile > SIP Trunk Security Profile**.

Step 2 To add a new profile, click **Add New** at the bottom of the page or click the **+** sign at the top of the page.

Step 3 Enter the settings as indicated in Table 16-7 to configure the SIP trunk security profile.

Step 4 To save your configuration, click **Save**.

Table 16-7 SIP Trunk Security Profile Settings

Field	Required	Setting
Name	Yes	Enter a text string that identifies this SIP trunk security profile.
Description	—	Enter a text string that describes this SIP trunk security profile.
Device Security Mode	Yes	Drop-down list. Choose **Encrypted**.
Incoming Transport Type	Yes	Drop-down list. Choose **TCP+UDP**.
Outgoing Transport Type	Yes	Drop-down list. Select **TCP**.
X.509 Subject Name	Yes	Enter the subject name of the Cisco TelePresence Multipoint Switch Root Certificate that you noted in Step 7 of the previous procedure.
Incoming Port	Yes	Enter **5060** for non-secure trunk. If using SIP security, enter a different unused port (such as 5275).

Setting Cisco TelePresence Multipoint Switch as Secure

Procedure

To set the Cisco TelePresence Multipoint Switch as secure, do the following procedure:

Step 1 Choose **Configure > Security Settings**.

Step 2 In the Meeting Security Policy field, choose **Best Effort**.

Step 3 Click **Apply**.

Step 4 Choose **Configure > Cisco Unified CM**.

The Unified CM window is displayed.

Step 5 Click the **SIP Profile Settings** tab.

Step 6 From the Device Security drop-down list, select **Trusted Trunk** and check the Media Encryption check box.

Step 7 From the Transport Layer Protocol drop-down list, choose **TCP**.

Step 8 To save your changes, click **Apply**.

Step 9 After reading the notice that is displayed, click **OK**.

Step 10 To check the Meeting Security Policy of the static meetings on the system, choose **Manage > Static Meetings**.

The Static Meetings page is displayed. The Security Policy column indicates the value of the Meeting Security Policy field.

Step 11 If you have static meetings that have not been set up to use a Meeting Security Policy of Best-Effort, do the following sub-steps to edit the meetings.

d. Check the check box next to a meeting, and click **Edit**.

e. For Meeting Security Policy, select **Best-Effort**.

f. To save the modified setting, click **Apply**.

Configuring the Conference Control Protocol (CCP) VPN Security Solution

The Cisco TelePresence Multipoint Switch uses the Conference Control Protocol (CCP) to provide CTS endpoints with access to in-meeting functions, such as the participant list; room or speaker switching policies; and the lock meeting feature. CCP is delivered over HTTP or HTTPS.

The VPN security solution for CCP allows you to specify a default route (via an outbound http proxy) for CCP traffic, so that the traffic between the CTS and a remote CTMS can be routed hop-by-hop across one or more HTTP proxies.

In the CCP VPN model (fixed path) solution, the administrator configures the enterprise by adding a static (fixed path) configuration file to the Cisco Unified Communications Manager. When the CTS endpoint joins a meeting on the Cisco TelePresence Multipoint Switch, the endpoint attempts to route CCP traffic based on this configuration file. Typically, you set up the file so that all CCP HTTP traffic first attempts to go to a local CTMS. If no local CTMS matches, packet traffic is routed to the HTTP proxy.

Note This feature is only active if the enterprise configuration file is configured on the Cisco Unified Communications Manager TFTP server. If there is no TFTP configuration file present on the system, conference control uses the Internet model (free path).

Do the following tasks to configure the CCP VPN security solution:

1. Configure a proxy server, such as a Cisco Application Control Engine (ACE), to route the CCP traffic from the CTS to the remote Cisco TelePresence Multipoint Switch.

   Refer to the documentation of your specific proxy server for instructions, or see https://supportforums.cisco.com/community/netpro/collaboration-voice-video/telepresence/blog/2012/06/21/conference-control-protocol-ccp-for-telepresence-exchange-system for an example ACE configuration.

2. Create the cts-ccp-servers.txt configuration file.
3. Upload the configuration file to the Cisco Unified Communications Manager TFTP server.
4. Configure the External URL for the CCP service on the Cisco TelePresence Multipoint Switch.
5. Restart the CTS endpoint.
6. Join a meeting on the Cisco TelePresence Multipoint Switch and verify that the CCP HTTP traffic routes through the proxy server.

See the following topics for more information on the tasks:

- Creating the CCP VPN Configuration File, page 16-17
- Uploading the Configuration File to the Cisco Unified Communications Manager TFTP Server, page 16-17

- Configuring the External URL for the Cisco TelePresence Multipoint Switch, page 16-18
- Restarting the CTS Endpoint, page 16-18

Creating the CCP VPN Configuration File

The CCP VPN configuration file contains a list of local Cisco TelePresence Multipoint Switch servers and/or a default HTTP proxy in the format <IP address> [<hostname>]. Use a text file editor to create a file named **cts-ccp-servers.txt**.

The following text is an example of a cts-ccp-servers.txt file which specifies a list of local CTMS servers followed by the default HTTP proxy path for secure routing outside of the enterprise.

```
192.0.2.10        ctms-SanJose.example.com
192.0.2.20        ctms-RCDN.example.com
203.0.113.1       ctms-HK.example.com
# default
198.51.100.10     default
```

Uploading the Configuration File to the Cisco Unified Communications Manager TFTP Server

Procedure

Do the following procedure to upload the cts-ccp-servers.txt file to the Cisco Unified Communications Manager TFTP directory.

Step 1 Log in to the Cisco Cisco Unified Communications Manager Administration interface.

Step 2 From the Navigation drop-down menu in the upper right corner, choose **Cisco Unified OS Administration** and click **Go**.

Step 3 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades** > **TFTP File Management**.

The TFTP File Management window displays and shows a listing of the current uploaded files. You can filter the file list by using the Find controls.

Step 4 To upload the cts-ccp-servers.txt file, do the following substeps:

a. Click **Upload File**.

The Upload File dialog box opens.

b. To upload the file, click **Browse** and then choose the cts-ccp-servers.txt file.

c. To start the upload, click **Upload File**.

The Status area indicates when the file uploads successfully.

Step 5 After the file uploads, do the following substeps to restart the Cisco TFTP service:

a. From the Navigation drop-down menu in the upper right corner, choose **Cisco Unified Serviceability** and click **Go**.

b. Log in to Cisco Unified Serviceability.

c. From the Tools drop-down menu, choose **Control Center - Feature Services**.

d. From the Select Server drop-down menu, choose the TFTP server and click **Go**.

e. From the CM Services menu, click the **Cisco TFTP** radio button.

f. Click the **Restart** button.

g. Repeat Step c. through Step f. for all TFTP servers.

Configuring the External URL for the Cisco TelePresence Multipoint Switch

The external URL is an HTTP proxy URL that CTMS advertises to the CTS endpoints in a meeting. The URL enables a reverse proxy to parse requests for more than one CTMS, even though the CTS client uses a single default proxy IP address for all remote CTMS servers.

Procedure

Do the following procedure to configure the HTTP proxy URL.

Step 1 In the Cisco TelePresence Multipoint Switch Administration software, use the left navigation to choose **Services**.

The Services page displays.

Step 2 In the External URL field, enter the routable service location, in a format such as https://<proxy-default-ip-address>/<ServiceProvider-identifier>/<Enterprise-identifier>/<ctms-identifier>. For example, **https://198.51.100.10:9501/cisco/sj/ctms1**.

Step 3 Click **Apply**.

The Web UI automatically restarts all CTMS processes to have Confgmr/CCS reload the new URL.

Restarting the CTS Endpoint

When you restart the CTS, the endpoint downloads the configuration file from the Cisco Unified Communications Manager TFTP server. The endpoint performs error checking on the configuration file. If the file passes the error check, the CTS confctrl component loads the file when it comes up.

When the CTS comes up after the restart, check the SYSOP log to verify that the cts-ccp-server file was found. The log should include the following message: “CTS is configured with appropriate file to perform B2B conference control.”

Enabling Cisco TelePresence Endpoints Running TC Release 5.x to Join Meetings Hosted on the Cisco TelePresence Multipoint Switch

Cisco TelePresence endpoints running TC release 5.x require a configuration change to a default setting on Cisco TelePresence Multipoint Switch version 1.8 in order to join meetings hosted on the switch.

Procedure

To enable Cisco TelePresence TC5.x endpoints to join meetings hosted on the Cisco TelePresence Multipoint Switch, do the following procedure:

Step 1 From the left navigation pane, choose **Manage > Default Meeting Settings**.

The Default Settings window displays.

Step 2 For Supported Endpoint Types, select **Cisco TelePresence TC 5.0 (and later) and CTS 1.8 (and later) endpoints**.

Step 3 To save the modified setting, click **Apply**.

CHAPTER 17

Configuring the Cisco Router with IVR

A Cisco gateway router provides integrated voice response (IVR) functionality to the Cisco TelePresence Exchange System, thus providing greetings and voice prompts to conference participants.

This section describes the configuration that is required on the Cisco gateway router to provide IVR functionality, and includes the following topics:

For supported router models and Cisco IOS software requirements, see the applicable *Release Notes for Cisco TelePresence Exchange System*, at http://www.cisco.com/go/ctx-relnotes.

For additional details about configuring SIP, see the *Cisco IOS SIP Configuration Guide, Release 15.1M&T*, at http://www.cisco.com/en/US/docs/ios-xml/ios/voice/sip/configuration/15-1mt/sip-15-1mt-book.html.

Downloading Application Files from the FTP Server

In order for the IVR router to provide prompts for Meet-Me and Rendezvous meetings, you must copy the meetme.tcl file to the router. You can download the Meet-Me application file from the TelePresence Exchange Products section of the Cisco TelePresence Downloads page at http://www.cisco.com/cisco/software/navigator.html?mdfid=280789323&flowid=25321.

To copy the Meet-Me application file to the IVR router, use the following command:

```
Router # copy ftp:// <user>:<password>@<host>/<path_to_file> flash:
```

where

User is the login username for the FTP server on which you download the *meetme-tcl* file.

Password is the login password for the FTP server.

Host is the hostname or IP address of the FTP server.

Path_to_file is the full path to the *meetme.tcl* file on the home directory of the FTP server.

Flash is the local directory in which the system copies the file.

Configuring the Router to Pass SIP Headers

Procedure

To configure the router to pass the SIP headers to the VXML application, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# voice service voip`	Enters voice service configuration mode for VoIP.
Step 2	`Router(config-voi-srv)# sip`	Enters Session Initiation Protocol (SIP) configuration mode.
Step 3	`Router(config-serv-sip)# header-passing`	Enables passing of headers in the SIP INVITE, SUBSCRIBE, and NOTIFY messages.
Step 4	`Router(config-serv-sip) exit`	Exits SIP configuration mode.

The following example configures the IVR service to pass the message headers:

```
Router(config)# voice service voip
Router(config)# sip
Router(config)# header-passing
```

Configuring Application Parameters

Procedure

To configure an application on the router, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# application`	Enters application configuration mode.
Step 2	`Router(config-app)# service` *application-name location*	Configures a specific application on a dial peer. Location is the directory and file name of the Tcl script for the application.
Step 3	`Router(config-app)# monitor`	Enters monitor configuration mode.
Step 4	`Router(config-app-monitor)# interface stats`	Enables statistics monitoring for the interface.
Step 5	`Router(config-app-monitor)# interface event-log`	Enables event logging for the interface.
Step 6	`Router(config-app-monitor) stats`	Enables statistics collection.
Step 7	`Router(config-app-monitor)# event-log`	Enables event logging for the voice application.

The following example configures the Meet-Me service:

```
Router(config)# application
Router(config-app)# service meet_me flash://meetme.tcl
Router(config-app)# monitor
Router(config-app-monitor)# interface stats
Router(config-app-monitor)# interface event-log
Router(config-app-monitor)# stats
Router(config-app-monitor)# event-log
```

Configuring VOIP Dial Peers

Procedure

To define a dial peer, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice tag voip`	Defines a VoIP dial peer. Tag is a locally unique number.
Step 2	`Router(config-dial-peer)# application application-name`	Specifies the application for the dial peer.
Step 3	`Router(config-dial-peer)# session protocol sipv2`	Specifies a session protocol for use between the peers.
Step 4	`Router(config-dial-peer)# incoming called-number string`	Configures the expected digit string for incoming called numbers. **Note** The called-number must match the ivr_nb that is configured in the Cisco TelePresence Exchange System. The default value is 3666.
Step 5	`Router(config-dial-peer)# dtmf-relay rtp-nte sip-kpml`	Specifies how to relay dual-tone multi-frequency (DTMF) tones to the peer. The rtp-nte keyword tells the router to forward DTMF tones by using the real-time protocol (RTP) with the Named Telephone Event (NTE) payload type. The sip-kpml keyword tells the router to forward DTMF tones through Keypad Markup Language (KPML) messages.
Step 6	`Router(config-dial-peer)# codec codec`	Specifies the voice codec rate of speech for a dial peer.

The following example configures the VoIP dial peer for the Meet-Me service:

```
Router(config)# dial-peer voice 100 voip
Router(config-dial-peer)# service meet_me
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# incoming called-number 3666
Router(config-dial-peer)# dtmf-relay rtp-nte
Router(config-dial-peer)# codec g711ulaw
```

CHAPTER 18

Configuring Cisco Unified Communications Manager

The procedures in this section address the minimum configuration requirements necessary on Cisco Unified Communications Manager (Unified CM):

- Create a SIP trunk security profile. This security profile will be used on the SIP trunk between the Unified CM and the Cisco Session Border Controller (SBC).
- Create a SIP profile for Binary Floor Control Protocol (BFCP) support. This profile will be associated with the phone devices that use BFCP for presentation sharing, and with the SIP trunk between Unified CM and the SBC.
- Create a Session Initiation Protocol (SIP) trunk. The SIP trunk is used for communication between Unified CM and the SBC.
- Create route patterns. A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns are used for routing conference numbers to the media bridge resources that support dial-in calls.

The procedures in this section assume that the Unified CM is already active in the network. For minimum software requirements for the Unified CM, see the applicable *Release Notes for the Cisco TelePresence Exchange System*, at http://www.cisco.com/go/ctx-relnotes.

Additional configuration steps for the Unified CM, can be found at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

This section includes the following topics:

Logging into the Cisco Unified Communications Manager Administration Application

Procedure

To log into the Unified CM Administration application, do the following procedure:

Step 1 Access a web browser that is supported by the Unified CM Administration application from any user PC in your network. In the address bar of the web browser, enter the following URL:

`https://Unifed_CM-server-name`

where *Unified_CM-server-name* is the name or IP address of the server.

Note If your network uses DNS services, you can specify the hostname of the server where Unified CM is installed. If your network does not use DNS services, you must specify the IP address of the server.

Step 2 Log in with your assigned administrative privileges.

Step 3 From the Navigation field at the upper right corner of the page, click **Cisco Unified Communications Manager Administration**, and then click **Go**.

The system returns to the Cisco Unified Communications Manager Administration home page.

Creating a SIP Trunk Security Profile

Procedure

To create a SIP trunk security profile, do the following procedure:

Step 1 Click **System**. Under **Security Profile**, click **SIP Trunk Security Profile**.

Step 2 Click **Add New** at the bottom of the page or click the **+** sign at the top of the page.

Step 3 Enter the settings as indicated in Table 18-1 to configure the SIP trunk security profile. Leave default settings for fields not included in Table 18-1.

Step 4 To save your changes, click **Save** at the bottom of the page.

Table 18-1 SIP Trunk Security Profile Settings

Field	Required	Setting
Name	Yes	Enter a text string that identifies this SIP trunk security profile.
Description	—	Enter a text string that describes this SIP trunk security profile.

Table 18-1 SIP Trunk Security Profile Settings (continued)

Field	Required	Setting
Device Security Mode	Yes	Choose **Encrypted**.
Incoming Transport Type	Yes	TLS will be entered automatically.
Outgoing Transport Type	Yes	Choose **TCP**.
X.509 Subject Name	Yes	Enter the subject name of the Cisco TelePresence Multipoint Switch Root Certificate.
Incoming Port	Yes	Enter **5060** for non-secure trunk. If using SIP security, enter a different unused port (such as 5275).

Creating a SIP Profile for BFCP

Binary Floor Control Protocol (BFCP) enables SIP endpoints to do presentation sharing. The use of BFCP creates an additional media stream in addition to the existing audio and video streams. This additional stream is used to stream a presentation, such as a PowerPoint presentation from a laptop, into a SIP endpoint.

Note BFCP is only supported on SIP networks. BFCP must be enabled on all SIP trunks, lines, and endpoints for presentation sharing to work. BFCP is not supported if the SIP line or SIP trunk uses MTP, RSVP, TRP or Transcoder.

Procedure

To create a SIP profile for use with endpoints that allow BFCP presentation sharing, do the following procedure:

Step 1 Click **Device**. Under **Device Settings**, click **SIP Profile**.

Step 2 Click **Add New** at the bottom of the page or click the **+** sign at the top of the page.

Tip If you already have a SIP profile you want to use for endpoints, locate the profile and modify it according to the rest of this procedure.

Step 3 Enter the settings as indicated in Table 18-2 to configure the SIP profile. Leave default settings for fields not included in Table 18-2.

Step 4 To save your changes, click **Save** at the bottom of the page.

Step 5 Apply the SIP profile to the endpoint devices. For instructions, see the applicable *Cisco Unified Communications Manager Administration Guide* for your release, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Table 18-2 SIP Profile Settings

Field	Setting
SIP Profile Information	
Name	Enter a text string that identifies this SIP trunk security profile.
Description	Enter a text string that describes this SIP trunk security profile.
Allow Presentation Sharing using BFCP	Check the check box.
Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on	Choose **Never**.
RSVP Over SIP	Choose **Local RSVP**.
Fall Back to Local RSVP	Check the check box.
SIP Rel1XX Options	Choose **Disabled**.
Deliver Conference Bridge Identifier	Uncheck the check box.
Early Offer support for voice and video calls (insert MTP if needed)	Uncheck the check box.
Send send-receive SDP in mid-call INVITE	Uncheck the check box.

Creating a SIP Trunk

You must configure a SIP trunk for communication between Unified CM and the SBC.

Procedure

To create a SIP trunk, do the following procedure:

Step 1 Log in to the Unified CM Administration portal as the ccmadministrator user.

Step 2 Choose **Device > Trunk** and click **Add New**.

Step 3 At the New Trunk Configuration page, do the following:

a. From the Trunk Type drop-down menu, select **SIP Trunk,** and then click **Next**.

The Device Protocol field updates and displays SIP.

b. In the Device Name field, enter a name for the SIP trunk.

c. In the Description field, enter a description for the SIP trunk.

d. Select a Device Pool option other than the Default option.

If there are multiple device pools, contact your system administrator to determine the appropriate device pool selection.

e. Scroll down to the SIP Information section of the window, and enter the SBC ingress IP address in the Destination Address field. The SBC will forward traffic to the Cisco TelePresence Exchange System.

f. From the SIP Trunk Security Profile drop-down menu, select **Non Secure SIP Trunk Profile**.

g. From the SIP Profile drop-down menu, if you are not using BFCP, select **Standard SIP Profile**. Otherwise, select the SIP profile that you configured in the "Creating a SIP Trunk Security Profile" section on page 18-2.

h. To create the SIP Trunk, click **Save**.

Associating the SIP Trunk with Route Patterns

After you define a SIP Trunk on Unified CM, you must associate the SIP Trunk with the appropriate route patterns to the SBC.

You must configure two types of route patterns:

- A route pattern for an IVR access number

  In this case, the caller knows the Meet-Me phone number but does not know the Meet-Me meeting ID. Therefore, Unified CM forwards the call to the Cisco AS5350XM (IVR resource server) to retrieve and play the IVR files.

- A route pattern for the One-Button-to-Push (OBTP) access number

  In this case, the caller is able to place OBTP calls because the caller knows both the Meet-Me access number and the Meeting ID.

Procedure

To create route patterns to the SBC, do the following procedure:

Step 1 Log in to the Unified CM Administration portal as the ccmadministrator user.

Step 2 Choose **Call Routing > Route/Hunt > Route Pattern**.

Step 3 At the Find and List Route Pattern window, click **Add New**.

The Route Pattern Configuration window is displayed.

Step 4 To create an IVR access number, do the following:

a. In the Route Pattern field, enter the IVR access number.

   The format for the IVR number is the access number only as seen in the following example:

   18006338631

b. Select the **SIP Trunk** from the Gateway/Route List drop-down menu that routes to the SBC.

c. Check the **Urgent Priority** check box.

d. To save the change, click **Save**.

Step 5 To create an OBTP access number, do the following:

a. Click **Add New**.

   The Route Configuration Window is displayed.

b. In the Route Pattern field, enter the OBTP access number.

   The format for the OBTP number is the access number followed by two asterisks followed by a meeting ID wildcard value that is represented by eight *X*s as seen in the following example:

*18006338631**XXXXXXXX*

c. From the Gateway/Route List drop-down menu, select the **SIP Trunk**.

d. To save your changes, click **Save**.

Note The Unified CM configuration in your network might require additional configuration of the route pattern to ensure it operates properly within your network. Check with your system administrator for other requirements.

Route pattern configuration fields are shown in Table 18-3.

Table 18-3 Route Pattern Configuration Settings

Field	Required	Setting
Pattern Definition		
Route Pattern	Yes	Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. The uppercase characters A, B, C, and D are valid characters. **Note** The route pattern that is configured must match the access settings numbers that are configured in the Cisco TelePresence Multipoint Switch.
Description	—	A text string that describes this route pattern.
Gateway/Route List	Yes	Select the SIP trunk that you created for Cisco TelePresence Multipoint Switch.
Call Classification	Yes	Choose **OnNet**.

Deleting a Unified CM from the Cisco TelePresence Exchange System Administration Console

Procedure

To delete a Unified CM from the Cisco TelePresence Exchange System, do the following procedure:

Step 1 From the navigation pane of the Cisco TelePresence Exchange System administration console, choose **Media Resources > Unified CM Resources**.

The Unified CM Resources window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple Unified CM resources at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a Unified CM resource prior to deleting it, in the Unified CM Resources window, you can click the applicable **Unified CM resource** to go to the Unified CM Resources page. After verifying that you have chosen the correct Unified CM resource to delete, click **Delete This Unified CM Resource**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

CHAPTER 19

Configuring Cisco TelePresence Manager

This section describes the configuration steps necessary for the Cisco TelePresence Manager to communicate with the Cisco TelePresence Exchange System.

The procedures in this section assume that the Cisco TelePresence Manager is installed and active in the network. For minimum software requirements for the Cisco TelePresence Manager, see the applicable *Release Notes for the Cisco TelePresence Exchange System*, at http://www.cisco.com/go/ctx-relnotes.

If you are installing this system for the first time, see the "Initializing Cisco TelePresence Manager" chapter in the *Cisco TelePresence Manager Release 1.8 Administration and Installation Guide* for step-by-step instructions. The guide is available at http://www.cisco.com/en/US/docs/telepresence/cts_manager/1_8/admin/ctm1_8adminguide.html.

Note To ensure proper interoperability between the Cisco TelePresence Manager and the Cisco TelePresence Exchange System, a Cisco support engineer must perform additional configuration to enable the API on the Cisco TelePresence Manager and to enable the hosted mode for OBTP functionality. To arrange for this support, contact your local Cisco system engineer or file a support case at Cisco.com.

Be aware that if the necessary configuration is not done, the Cisco TelePresence Exchange System might fail to authenticate with the Cisco TelePresence Manager or might report the following API exception value and cause code: ERC_CTSMAN_COMMUNICATION_FAILURE (exception value), CTSMAN_INTERCOMPANY_NOT_CONFIGURED (cause code).

This section includes the following topics:

Configuring Lightweight Directory Access Protocol Servers

Procedure

To configure Lightweight Directory Access Protocol (LDAP) servers, do the following procedure:

Step 1 Log in to the Cisco TelePresence Manager web portal as the administrator.

Step 2 Choose **Configure > LDAP Server**.

Step 3 To add a new LDAP server, click **New**.

The LDAP Server entry window is displayed.

Step 4 At the LDAP server window, enter values in the LDAP Servers window as described in Table 19-1.

Step 5 After verifying the connection to the LDAP server by clicking **Test Connection**, select **Save**.

Step 6 To verify that the newly defined LDAP Server appears as a defined server in the summary list on the page, click **Refresh** on the LDAP Server window.

Step 7 To add an additional LDAP Server, repeat Step 3 through Step 6.

Table 19-1 LDAP Server Settings

Field or Button	Description or Setting
Host	The LDAP server hostname.
Bind Method	Select the applicable radio button to select the binding method: • Normal—Cisco TelePresence Manager communicates with the LDAP server in clear text by using HTTP. • Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. **Note** To operate with the Cisco TelePresence Exchange System, select **Normal**.
Port	Enter the applicable port given the configuration: • The default port for a normal connection in a single LDAP server deployment is 389. • The default port for a secure connection is 636. **Note** To operate with the Cisco TelePresence Exchange System, use the default port value of 389.
Default Context	Refers to the default context from which the LDAP queries are performed. To change the context string, click **Fetch Distinguished Names** and choose the context from the Fetch DNS drop-down list adjacent to this field. **Note** To operate with Cisco TelePresence Exchange System, click **Fetch Distinguished Names**.

Table 19-1 LDAP Server Settings (continued)

Field or Button	Description or Setting
Username	Refers to the username that is used to authenticate the LDAP server. This must be in the LDAP fully qualified domain name (FQDN) format. Example: cn=administrator,cn=users, dc=<mydomain>, dc=com Another example is cn=CTSMan User. The Cisco TelePresence Manager Active Directory configuration requires using users that have the Domain Admin privilege. The user, CTSMan User, needs to be created with only the Domain Users privilege.
Append default context	When you check the check box next to the username, it appends the default context to the username. **Note** To operate with Cisco TelePresence Exchange System, check the **Append default context** check box.
Password	Refers to the LDAP server password.
Certificate	Refers to the name of the LDAP certificate. **Note** You do not need to select this option unless you chose the Secure Bind Method. The Cisco TelePresence Exchange System uses the Normal Bind Method, so you do not need to enter the certificate.
User Containers	Describes values for user and meeting room information that the Cisco TelePresence Manager retrieves from the LDAP Server. Additionally, these containers are used to retrieve user information for authentication from the LDAP server. You can specify more than one user container. **Note** If you have an LDAP peer domain configured, you need to specify its user containers and context. For example, cn=users, dc=domain2, dc=com. When specifying the container and context information for your peer domain, you do not check the Append default context box.
Append default context	Refers to a check box next to the Users Containers field. When you check the Append default context check box, it appends the default context to the User Container. **Note** To operate with Cisco TelePresence Exchange System, check the **Append default context** check box.
Test Connection	Tests the connection between the Cisco TelePresence Manager and the LDAP server.

Configuring Unified CM

The following sections describe how to configure the Cisco Unified CM:

- Adding a User Group, page 19-4
- Assigning Roles to a User Group, page 19-4
- Creating an Application User, page 19-5

Adding a User Group

Procedure

To add a user group to the Cisco Unified CM, do the following procedure:

Step 1 From the **Cisco Unified CM Administration** page, choose **User Group** from the **User Management** drop-down menu.

Step 2 Click **Add New**.

Step 3 Enter a name for the new user group.

Step 4 Click **OK**.

Step 5 To save the configuration, click **Save**.

Assigning Roles to a User Group

Procedure

To assign roles to a user group in Cisco Unified CM, do the following procedure:

Step 1 From the **Cisco Unified CM Administration** page, choose **User Group** from the **User Management** drop-down menu.

Step 2 Click the name of the user group for which you want to assign roles.

Step 3 From the Related Links drop-down list box, choose **Assign Role to User Group**.

Step 4 Click **Go**.

Step 5 Click **Assign Role to Group**.

Step 6 Choose the following roles to assign to this user group by clicking the check boxes next to the role names:

- Standard AXL API Access
- Standard CTI Enabled
- Standard Serviceability
- Standard CCM Admin Users

Step 7 Click **Add Selected**.

Step 8 To save the configuration, click **Save**.

Creating an Application User

Procedure

To create an application user in Cisco Unified CM, do the following procedure:

Step 1 From the **Cisco Unified CM Administration** page, choose **Application User** from the **User Management** drop-down menu.

Step 2 Click **Add New**.

Step 3 Complete all necessary Application User Information fields.

Step 4 To save your configuration, click **Save**.

Adding Users to a User Group

Procedure

To add application users to a user group in Cisco Unified CM, do the following procedure:

Step 1 From the **Cisco Unified CM Administration** page, choose **User Group** from the **User Management** drop-down menu.

Step 2 Click the name of the user group that you want to update.

Step 3 To add application users, click **Add App Users to Group**.

Step 4 Click the check box next to the application users that you want to add to this user group.

Step 5 Click **Add Selected**.

Step 6 To save the configuration, click **Save**.

Downloading the Certificate

To enable an HTTPS connection to the Unified CM, you must download a certificate that identifies the server during the connection process.

You can accept the server certificate for the current session only, or you can download the certificate to a trusted folder (file) to secure the current session and future sessions with that server. The trusted folder stores the certificates for all your trusted sites.

Cisco supports the following browsers for connection to the Cisco Tomcat web server application in Cisco Unified Communications Manager:

- Internet Explorer 6 or later
- Mozilla 3.0 or later

Note In this procedure, the steps for the Firefox Mozilla browser are shown. For specific details on downloading a certificate using Internet Explorer, see the "Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)" section in the *Cisco Unified Communications Manager Security Guide*, at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/8_6_1/secugd/sec-861-cm.html.

Procedure

To save the HTTPS certificate in the trusted folder, do the following procedure:

Step 1 From a new browser window, navigate to your Unified CM by entering the hostname, local host, or IP address for the Cisco Unified Communications Manager Administration web portal.

Step 2 Choose **Tools > Page Info**.

Step 3 When the Security Alert dialog box is displayed, click **View Certificate**.

The Certificate window is displayed.

Step 4 To view the details of the certificate, select the **Details** tab.

Step 5 From the Certification window, click **Export**.

Note When using Mozilla Firefox, save the certificate in the DER format.

Uploading the Certificate to Cisco TelePresence Manager

Procedure

To upload the certificate from the trusted folder onto the Cisco TelePresence Manager server, do the following procedure:

Step 1 From the Cisco TelePresence Manager, choose **Configure > Unified CM**.

Step 2 Click **New**.

Step 3 To add a new Unified CM Service, enter the values as described in Table 19-2.

Step 4 To save the configuration, click **Save**.

Step 5 To verify the addition of the new Unified CM Service, click **Refresh** on the Unified CM window.

Table 19-2 Unified CM Service Values

Field or Button	Description or Setting
Host	The Unified CM hostname.
Username	The application user name on the Unified CM. This is the user name that you created in the "Creating an Application User" section on page 19-5.
Password	The password for the application user name.

Table 19-2 Unified CM Service Values (continued)

Field or Button	Description or Setting
Certificate	Certificate file. Browse to locate the certificate in the trusted folder.
Save	Saves the entry.

Configuring the Scheduling API

The Cisco TelePresence Exchange System uses the Scheduling API to obtain information from the Cisco TelePresence Manager about hosted rooms.

You can configure the Scheduling API during Cisco TelePresence Manager initialization (see Table 19-3 for configuration values) or you can configure at a later date by accessing the **Configure > Scheduling API** window of the Cisco TelePresence Manager as detailed in the procedure below.

Procedure

To configure the Scheduling API, do the following procedure:

Step 1 From the Cisco TelePresence Manager Administration Portal, choose **Configure > Scheduling API**.

Step 2 To configure the Scheduling API, enter values in the Scheduling API window as described in Table 19-3.

Step 3 To verify the connectivity, click **Verify**.

Step 4 To save the configuration, click **Apply**.

Table 19-3 Scheduling API Settings

Field or Button	Description or Setting
Host	Enter 1.1.1.1 in the hostname field. A hostname is not necessary.
Bind Method	Select the applicable radio button to select the binding method: • Normal—Cisco TelePresence Manager communicates with the LDAP server in clear text by using HTTP. • Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. **Note** To operate with the Cisco TelePresence Exchange System, select **Normal**.
Port	Enter the HTTP default port number of 80.
Logon Name	Logon Name is in the email format of LDAP servers, for example, ctsmanager@yourcompany.com.
Password	The password that is associated with the logon name.

Table 19-3 Scheduling API Settings (continued)

Field or Button	Description or Setting
Certificate	*Available only if the secure bind method is selected.* Click **Choose File** to select the certificate.
Test Connection	Tests the connection between the Cisco TelePresence Manager and the LDAP server. **Note** You must configure the Cisco TelePresence Manager as a resource in the Cisco TelePresence Exchange System Administration Console before you can test the connection. See the "Configuring CTS Manager Resources" section in the "Configuring Endpoints" chapter.

Adding Licenses

You must configure the following licenses on the Cisco TelePresence Manager:

- Room Handling License

  The Room Handling License is a count-based license. Count-based licenses are based on the number of rooms (with a telepresence system). Each telepresence system subscribes to a license. The count-based license is available in 10-room, 50-room, and 100-room license groups.

- Scheduling API License

  For the Scheduling API, the license is enforced at the API call. When a client makes an API call, Cisco TelePresence Manager returns the response if a valid license exists. If a license does not exist, a License-not-found error is returned.

Procedure

To configure the Room and Scheduling API licenses, do the following procedure:

Step 1 From the Cisco TelePresence Manager, choose **Configure > Licenses > Licences Files**.

The Licenses Files window displays licenses that are already loaded on the system.

Step 2 To find the license file to upload, click **Upload**.

The License Upload window is displayed.

Step 3 At the License Upload window, click **Browse** to find the appropriate license file, and then click **Open**.

Step 4 To upload the license file, click **Upload**.

Step 5 To verify that your license uploads properly, click the **Summary** tab.

A status of LICENSE_VALID indicates a successful upload.

Enabling Intercompany Calls

Enabling the intercompany setting allows you to schedule meetings between organizations. After you enable the intercompany setting, it cannot be disabled.

The Provider setting allows you to select either Another Company Hosts or Our Company Hosts. You cannot select both. You can change this setting depending on whether the company is going to host a meeting or be hosted. If multiple occurring meetings are set up with the company that is acting as host, this company will be the host for all of the meetings.

Another Company Hosts

If you select this feature, this allows another company to set up telepresence meetings. You must provide the host with information on the number of rooms that will be participating in the telepresence calls.

Our Company Hosts

If your company is hosting the meeting, the person setting up the meetings needs to reserve the rooms and obtain dial-in and room information from the other company before setting up the telepresence meeting.

Procedure

Step 1 To enable intercompany features, choose **Configure > Application Settings**.

Step 2 Select the **Conference Bridges** tab.

Step 3 In the Intercompany section of the Conference Bridges window:

a. Enable Intercompany by clicking the **Yes** radio button.

b. Check the **Our Company Hosts** check box as the Provider option.

   Do not select any options other than Our Company Hosts.

Step 4 To save the configuration changes, click **Apply**.

Step 5 In the warning dialog box that is displayed, click **OK** to accept the configuration change.

CHAPTER 20

Configuring Cisco Session Border Controllers

This section describes the Cisco TelePresence Exchange System configuration requirements for the session border controller (SBC) functionality.

This section includes the following topics:

The procedures in this section assume that a Cisco Aggregation Series Router (Cisco ASR) serves as an SBC, and that the router is installed and active in the network. See the *Release Notes for the Cisco TelePresence Exchange System* document for information about the Cisco routers that support SBC functionality. The document is available at http://www.cisco.com/go/ctx-relnotes.

For more information about configuring the SBC on the Cisco ASR, see the *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* document at http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/2_xe/sbcu_2_xe_book.html.

For more details on the commands shown in the configuration commands below, see the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* document at http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html.

Note Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be referenced in this document as the session border controller (SBC).

Creating a Session Border Controller Interface

You must create an SBC interface for each SBC module in the Cisco ASR and assign at least one primary IP address to the interface.

Procedure

To configure the SBC interface, do the following procedure:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# interface sbc` *interface-number*	Creates a virtual SBC interface on the Cisco ASR.
Step 3	`Router(config-if)# ip address` *{IPv4 ip address} {IPv4 subnet address}*	Assigns a primary IP address and subnet mask to the SBC interface.
Step 4	`Router(config-if)# ip address` *{IPv4 ip address} {IPv4 subnet address}* **secondary**	(Optional) Assigns a secondary IP address and subnet mask to the SBC interface.

The following example shows how to create an SBC interface and assign primary and secondary IP addresses and subnet masks:

```
Router(config)# interface sbc 1
Router(config-if)# ip address 10.22.141.100 255.255.255.248
Router(config-if)# ip address 10.22.141.101 255.255.255.248 secondary
Router(config-if)# ip address 10.22.141.102 255.255.255.248 secondary
```

Creating a Management Interface

You must define at least one management interface on the Cisco ASR for Telnet and SSH remote access.

Procedure

To define a management interface, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# GigabitEthernet` *module* **/** *slot* **/** *port*	Enters interface configuration mode for the specified interface.
Step 2	`Router(config-if)# ip address` *{IPv4 ip address} {IPv4 subnet address}*	Assigns an IP address and subnet mask to the management interface.
Step 3	`Router(config-if)# negotiation auto`	Enables negotiation of the speed, duplex mode, and flow control on the Gigabit Ethernet interface.

The following example shows how to configure a management interface:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.22.139.84 255.255.255.224
Router(config-if)# negotiation auto
```

Creating the SBC Instance

To configure the signaling border element (SBE) and data border element (DBE) on the SBC, you first create an SBC instance.

Procedure

To create the SBC instance, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# sbc service-name`	Creates the SBC instance and enters SBC configuration mode.
Step 2	`Router(config-sbc)# sbe`	Enters SBE configuration mode.
Step 3	`Router(config-sbc-sbe)# secure-media`	Enables media pass through, which configures the SBC to treat every media flow as an encrypted media flow. This action enables DTLS and SRTP media packets to pass through the SBC.

The following example shows how to create the SBC instance and enable secure media pass through:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# secure-media
```

Configuring the Signaling Border Element

You configure the signaling border element (SBE) to enable SIP signaling functionality such as header and method profiles, header editors, adjacencies, call admission control policies, route tables and blacklists.

SBE configuration is described in the following sections:

Configuring Default Profiles

Procedure

To configure the default profiles on the SBE, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# sbc service-name`	Enters SBC configuration mode for the specified SBC instance.
Step 2	`Router(config-sbc)# sbe`	Enters SBE configuration mode.

	Command	Purpose
Step 3	`Router(config-sbc-sbe)#` **sip-header profile** *profile-name*	Configures a header profile for the SBE. Enter **default** as the profile-name to configure the default header profile. The default profile is used for all adjacencies that do not have a specific profile configured.
Step 4	`Router(config-sbc-sbe-mep-hdr)#` **blacklist**	Configures this editor to be a blacklist. **Note** By default, editors are whitelists.
Step 5	`Router(config-sbc-sbe-sip-hdr)#` **header** *header-name*	Adds the specified header to the profile.
Step 6	`Router(config-sbc-sbe-sip-hdr-ele)#` **action pass** {**add-first-header** | **add-header** | **as-profile** | **drop-msg** | **pass** | **replace-name** | **replace-value** | **strip**}	Configures the action to take on the header. For the Cisco TelePresence Exchange System configuration, always set the action **pass**, which allows the message to proceed. You also need to set the action to **replace-value**, which replaces the header content (value).
Step 7	`Router(config-sbc-sbe-sip-hdr-ele)#` **exit** `Router(config-sbc-sbe-sip-hdr)#` **exit**	Exits the header profile configuration mode.
Step 8	`Router(config-sbc-sbe)#` **sip method-profile default**	Configure a method profile for the SBE. Enter **default** as the profile-name to configure the default method profile. The default profile is used for all adjacencies that do not have a specific profile configured.
Step 9	`Router(config-sbc-sbe-sip-mth)#` **pass-body**	Permits SIP message bodies to pass through.
Step 10	`Router(config-sbc-sbe-sip-mth)#` **method** *method-name*	Adds a method with a specified name to a SIP message profile.
Step 11	`Router(config-sbc-sbe-sip-mth)#` **action pass**	Configures the action to take for the message. For the Cisco TelePresence Exchange System configuration, always set the action to **pass**, which allows the message to proceed.
Step 12	`Router(config-sbc-sbe-sip-mth)#` **exit**	Exits the method profile configuration mode.
Step 13	`Router(config-sbc-sbe)#` **sip option-profile default**	Configures the default SIP option profile for either a SIP option white list or black list profile on the SBE.
Step 14	`Router(config-sbc-sbe-sip-opt)#` **option** *opt-name*	Adds an option to the profile.
Step 15	`Router(config-sbc-sbe-sip-opt)#` **exit**	Exits the option profile configuration mode.

The following example shows how to define default header and method profiles:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip-header profile default
Router(config-sbc-sbe-mep-hdr)# blacklist
Router(config-sbc-sbe-sip-hdr-prf)# header Allow entry 1
Router(config-sbc-sbe-sip-hdr-prf-ent)# action pass
Router(config-sbc-sbe-sip-hdr-prf)# header Min-SE entry 1
Router(config-sbc-sbe-sip-hdr-prf-ent)# action pass
Router(config-sbc-sbe-sip-hdr-prf)# header Reason entry 1
Router(config-sbc-sbe-sip-hdr-prf-ent)# action pass
Router(config-sbc-sbe-sip-hdr-prf)# header SERVER entry 1
Router(config-sbc-sbe-sip-hdr-prf-ent)# action pass
```

```
Router(config-sbc-sbe-sip-hdr-prf)# header DIVERSION entry 1
Router(config-sbc-sbe-sip-hdr-prf-ent)# action pass
Router(config-sbc-sbe-sip-hdr-prf)# header Allow-Events entry 1
Router(config-sbc-sbe-sip-hdr-prf-ent)# action pass
Router(config-sbc-sbe-sip-hdr-prf)# header session-expires entry 1
Router(config-sbc-sbe-sip-hdr-prf-ent)# action replace-value value 1800
Router(config-sbc-sbe-sip-hdr-prf)# header RESOURCE-PRIORITY entry 1
Router(config-sbc-sbe-sip-hdr-prf-ent)# action pass
Router(config-sbc-sbe)# sip method-profile default
Router(config-sbc-sbe-sip-mth)# pass-body
Router(config-sbc-sbe-sip-mth)# method INFO
Router(config-sbc-sbe-sip-mth)# action pass
Router(config-sbc-sbe-sip-mth)# method REFER
Router(config-sbc-sbe-sip-mth)# action pass
Router(config-sbc-sbe-sip-mth)# method NOTIFY
Router(config-sbc-sbe-sip-mth)# action pass
Router(config-sbc-sbe-sip-mth)# method OPTION
Router(config-sbc-sbe-sip-mth)# action pass
Router(config-sbc-sbe-sip-mth)# method UPDATE
Router(config-sbc-sbe-sip-mth)# action pass
Router(config-sbc-sbe-sip-mth)# method SUBSCRIBE
Router(config-sbc-sbe-sip-mth)# action pass
Router(config-sbc-sbe)# sip-option profile default
Router(config-sbc-sbe-sip-opt)# option TIMER
Router(config-sbc-sbe-sip-opt)# option Require
Router(config-sbc-sbe-sip-opt)# option REPLACES
Router(config-sbc-sbe-sip-opt)# option Proxy-Require
Router(config-sbc-sbe-sip-opt)# exit
```

Configuring Editors

This section shows how to configure inbound and outbound SIP header editors for the SBC.

You must make sure that the SBC is not removing the contact header parameters that are required for the TC5 endpoints to connect to Cisco TelePresence Multipoint Switch (CTMS) meetings by using an interactive voice response (IVR) resource.

Procedure

To configure inbound and outbound SIP header editors, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)# sip header-editor` *editor-name*	Configures a header editor. You must specify the name of the header editor. For the Cisco TelePresence Exchange System configuration, specify an editor for both inbound and outbound.
Step 2	`Router(config-sbc-sbe-mep-hdr)# blacklist`	Configures this editor to be a blacklist. **Note** By default, editors are whitelists.
Step 3	`Router(config-sbc-sbe-mep-hdr)# store-rule` [**entry** *entry-number*]	Creates a store-rule context to extract variables from the headers. Specify the filtered entry number. By default, the value is 1.

	Command	Purpose
Step 4	`Router(config-sbc-sbe-mep-hdr-ele-act)# condition [comparison-type | boolean-operator | operator | comparison-value]`	Specifies one or more conditions for the action to be effective. Specify the *comparison-type* as the header-name *name* header-value that is used as the content of a different header. Specify the *operator* as [not] regex-match that is used for regular expression matching (BRE). Specify the *store-as* that is used to store rules only.
Step 5	`Router(config-sbc-sbe-mep-hdr-ele-act)# exit`	Exits the SIP header editor header action configuration mode.
Step 6	`Router(config-sbc-sbe-mep-hdr)# header header-name [entry entry-number]`	Adds a header to a SIP message editor. Specify the name of the header to be added to the header editor. Valid names are 1 to 32 characters in length (inclusive) and case-sensitive. Specify the filtered entry number. The range is from 1 to 99.
Step 7	`Router(config-sbc-sbe-mep-hdr-ele)# action {add-first-header| add-header | replace-name | replace-value} {value word}`	Configures an action to be taken on a header editor. You must add the first occurrence of a header (no action occurs if a header already exists). Then, specify the string that is used in conjunction with the action. The string is up to 256 characters. For the Cisco TelePresence Exchange System configuration, always set the action to **add-first-header** for the inbound editor and **replace-value** for both inbound and outbound editors.
Step 8	`Router(config-sbc-sbe-sip-hdr-ele-act)# condition [comparison-type | boolean-operator | operator | comparison-value]`	Specifies one or more conditions for the action to be effective. Specify the *comparison-type* as the variable that is used to match on variable content. Specify the *boolean-operator* as *is-defined* that is used to test if a variable is defined. Specify the *operator* as [not] eq that is defined as equals or not equal. Then, specify a character string or numeric value to compare.
Step 9	`Router(config-sbc-sbe-mep-hdr-ele-act)# exit` `Router(config-sbc-sbe-mep-hdr)#`	Exits the SIP header editor header action configuration mode and returns back to SIP header editor configuration mode.
Step 10	`Router(config-sbc-sbe-mep-hdr-ele)# action {as-editor | drop-msg | pass | strip}`	Configures an action to be taken on a header editor. For the Cisco TelePresence Exchange System configuration, always set the action to **strip** to delete the caller display name to avoid reporting issues from the TPS for both inbound and outbound editors.

The following example shows how to define inbound SIP header editors:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor in1
Router(config-sbc-sbe-mep-hdr)# blacklist
Router(config-sbc-sbe-mep-hdr)# store-rule entry1
Router(config-sbc-sbe-mep-hdr-ele-act)# condition header-name contact header-value
regex-match ";\(.*\)" store-as param
Router(config-sbc-sbe-mep-hdr-ele-act)# exit
Router(config-sbc-sbe-mep-hdr)# store-rule entry2
Router(config-sbc-sbe-mep-hdr-ele-act)# condition header-name session-expires header-value
regex-match ";\(.*\)" store-as refreshparam
Router(config-sbc-sbe-mep-hdr-ele-act)# exit
Router(config-sbc-sbe-mep-hdr)# header ctc-hdr-param entry 1
Router(config-sbc-sbe-mep-hdr-ele)# action add-first-header value "${param}"
Router(config-sbc-sbe-sip-hdr-ele-act)# condition variable param is-defined eq true
```

```
Router(config-sbc-sbe-mep-hdr-ele-act)# exit
Router(config-sbc-sbe-mep-hdr)# header remote-party-id entry 1
Router(config-sbc-sbe-mep-hdr-ele)# action strip
Router(config-sbc-sbe-mep-hdr)# header session-expires entry 1
Router(config-sbc-sbe-mep-hdr-ele)# action replace-value value 1800
Router(config-sbc-sbe-sip-hdr-ele-act)# condition variable refreshparam is-defined eq
false
Router(config-sbc-sbe-mep-hdr-ele-act)# exit
Router(config-sbc-sbe-mep-hdr)# header session-expires entry 2
Router(config-sbc-sbe-mep-hdr-ele)# action replace-value value “1800;${refreshparam}”
Router(config-sbc-sbe-sip-hdr-ele-act)# condition variable refreshparam is-defined eq true
Router(config-sbc-sbe-mep-hdr-ele-act)# exit
Router(config-sbc-sbe-mep-hdr)# header p-asserted-identity entry 1
Router(config-sbc-sbe-mep-hdr-ele)# action strip
Router(config-sbc-sbe-mep-hdr-ele)# exit
Router(config-sbc-sbe-mep-hdr)# header p-preferred-identity entry 1
Router(config-sbc-sbe-mep-hdr-ele)# action strip
```

The following example shows how to define outbound SIP header editors:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor out1
Router(config-sbc-sbe-mep-hdr)# blacklist
Router(config-sbc-sbe-mep-hdr)# store-rule entry1
Router(config-sbc-sbe-mep-hdr-ele-act)# condition header-name ctc-hdr-param header-value
store-as param
Router(config-sbc-sbe-mep-hdr-ele-act)# exit
Router(config-sbc-sbe-mep-hdr)# store-rule entry2
Router(config-sbc-sbe-mep-hdr-ele-act)# condition header-name contact header-value
regex-match "<\(.*\)>" store-as ctc
Router(config-sbc-sbe-mep-hdr-ele-act)# exit
Router(config-sbc-sbe-mep-hdr)# header contact entry1
Router(config-sbc-sbe-mep-hdr-ele)# action replace-value value "<${ctc}>;${param}"
Router(config-sbc-sbe-mep-hdr-ele-act)# condition variable ctc is-defined eq true
Router(config-sbc-sbe-mep-hdr-ele-act)# condition and variable param is-defined eq true
Router(config-sbc-sbe-mep-hdr-ele-act)# exit
Router(config-sbc-sbe-mep-hdr)# header contact entry2
Router(config-sbc-sbe-mep-hdr-ele)# action replace-value value "<${ctc}>"
Router(config-sbc-sbe-sip-hdr-ele-act)# condition variable ctc is-defined eq true
Router(config-sbc-sbe-sip-hdr-ele-act)# condition and variable param is-defined eq false
Router(config-sbc-sbe-mep-hdr-ele-act)# exit
Router(config-sbc-sbe-mep-hdr)# header ctc-hdr-param entry1
Router(config-sbc-sbe-mep-hdr-ele)# action strip
```

Creating Adjacencies

An adjacency represents a signaling relationship with a remote call agent. The adjacency defines protocol-specific parameters as well as admission control and routing policy. Each incoming call is matched to an adjacency, and each outgoing call is routed out over an adjacency.

You need to create adjacencies between the SBE and the following network elements:

- Cisco Application Control Engine
- Hosted Cisco Unified Communications Manager
- Both Cisco TelePresence Exchange System call engines

Also, you need to create an adjacency for each remote service provider to which we provide interconnect service.

Procedure

To create an adjacency, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)# adjacency (sip | h323) adjacency-name`	Enters configuration mode for the specified SIP or H.323 adjacency. For the Cisco TelePresence Exchange System configuration, enter **sip** as the type of adjacency.
Step 2	`Router(config-sbc-sbe-adj-sip)# nat force-off`	Configures network address translation (NAT) for the adjacency. **Note** The **nat force-off** option is the only supported option in this configuration. The **nat force-off** option sets the SIP adjacency to assume that all endpoints are not behind a NAT device.
Step 3	`Router(config-sbc-sbe-adj-sip)# editor-type {editor | profile}`	Specifies the editor type for the SIP adjacency to apply. For the Cisco TelePresence Exchange System configuration, always enter **editor** as the default for using the method, header, option, parameter, or body editor.
Step 4	`Router(config-sbc-sbe-adj-sip)# header-editor {inbound} {editor-name}`	Sets a specified header editor for inbound signaling on the SBE SIP adjacency. You must specify the name of the header editor to be set for inbound signaling on the adjacency.
Step 5	`Router(config-sbc-sbe-adj-sip)# header-editor {outbound} {editor-name}`	Sets a specified header editor for outbound signaling on the SBE SIP adjacency. You must specify the name of the header editor to be set for outbound signaling on the adjacency.
Step 6	`Router(config-sbc-sbe-adj-sip)# hunting-trigger error-codes`	Configures SIP to retry routing to the adjacency if it receives one of the specified error codes.
Step 7	`Router(config-sbc-sbe-adj-sip)# preferred-transport {tcp|udp}`	Sets the preferred transport protocol for SIP signaling on the adjacency.
Step 8	`Router(config-sbc-sbe-adj-sip)# signaling-address{ipv4_IP_address|ipv6_IP_address}`	Configures the local IP signaling address of the SIP adjacency.
Step 9	`Router(config-sbc-sbe-adj-sip)# statistics method summary`	Enables SIP method statistics on the adjacency.
Step 10	`Router(config-sbc-sbe-adj-sip)# signaling-port port-num [max-port-num]`	Configures the local port number for the signaling address of the SIP adjacency. Specify a maximum port number to configure a range of port values. The default port number is 5060.
Step 11	`Router(config-sbc-sbe-adj-sip)# remote-address ipv4 remote-address`	Restricts the set of remote signaling peers that can be contacted over the adjacency to those with the given IP address prefix. **Note** For Cisco TelePresence Exchange System configuration, enter the virtual IP (VIP) address of the Cisco ACE as the remote address.

	Command	Purpose
Step 12	`Router(config-sbc-sbe-adj-sip)#` **signaling-peer** *peer-name*	Configures the SIP adjacency to use the specified remote signaling-peer. Specify the IPv4 address of the signaling peer in dotted-decimal format. **Note** For Cisco TelePresence Exchange System configuration, enter the VIP address of the Cisco ACE as the signaling peer.
Step 13	`Router(config-sbc-sbe-adj-sip)#` **attach**	Attaches the adjacency to the SBC instance. The adjacency is now available for SIP call processing.

The following example shows how to create an adjacency between the SBE and the Cisco ACE:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SBC-ACE
Router(config-sbc-sbe-adj-sip)# nat force-off
Router(config-sbc-sbe-adj-sip)# editor-type editor
Router(config-sbc-sbe-adj-sip)# header-editor inbound in1
Router(config-sbc-sbe-adj-sip)# hunting-trigger 408 500 503
Router(config-sbc-sbe-adj-sip)# preferred-transport tcp
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 10.22.141.100
Router(config-sbc-sbe-adj-sip)# statistics method summary
Router(config-sbc-sbe-adj-sip)# signaling-port port-num 5060
Router(config-sbc-sbe-adj-sip)# remote-address ipv4 10.22.141.98 255.255.255.255
Router(config-sbc-sbe-adj-sip)# signaling-peer 10.22.141.98
Router(config-sbc-sbe-adj-sip))# attach
```

The following example shows how to create an adjacency between the SBC and the Unified CM and how to define a call admission control policy for the SBE:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip UNCM-SBC
Router(config-sbc-sbe-adj-sip)# nat force-off
Router(config-sbc-sbe-adj-sip)# editor-type editor
Router(config-sbc-sbe-adj-sip)# header-editor inbound in1
Router(config-sbc-sbe-adj-sip)# header-editor outbound out1
Router(config-sbc-sbe-adj-sip)# hunting-trigger 408 500 503
Router(config-sbc-sbe-adj-sip)# preferred-transport tcp
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 10.22.141.100
Router(config-sbc-sbe-adj-sip)# statistics method summary
Router(config-sbc-sbe-adj-sip)# signaling-port port-num 5060
Router(config-sbc-sbe-adj-sip)# remote-address ipv4 10.22.139.70 255.255.255.255
Router(config-sbc-sbe-adj-sip)# signaling-peer 10.22.139.70
Router(config-sbc-sbe-adj-sip)# attach
```

The following example shows how to create an adjacency between the SBC and the first Cisco TelePresence Exchange System call engine:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip sol1-ctc2-eng1
Router(config-sbc-sbe-adj-sip)# nat force-off
Router(config-sbc-sbe-adj-sip)# editor-type editor
Router(config-sbc-sbe-adj-sip)# header-editor inbound in1
Router(config-sbc-sbe-adj-sip)# hunting-trigger 408 500 503
Router(config-sbc-sbe-adj-sip)# preferred-transport tcp
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 10.22.160.104
Router(config-sbc-sbe-adj-sip)# statistics method summary
Router(config-sbc-sbe-adj-sip)# signaling-port 5060
```

```
Router(config-sbc-sbe-adj-sip)# remote-address ipv4 10.22.160.70 255.255.255.255
Router(config-sbc-sbe-adj-sip)# signaling-peer 10.22.160.70
Router(config-sbc-sbe-adj-sip)# attach
```

The following example shows how to create an adjacency between the SBC and the second Cisco TelePresence Exchange System call engine:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip sol1-ctc2-eng2
Router(config-sbc-sbe-adj-sip)# nat force-off
Router(config-sbc-sbe-adj-sip)# editor-type editor
Router(config-sbc-sbe-adj-sip)# header-editor inbound in1
Router(config-sbc-sbe-adj-sip)# hunting-trigger 408 500 503
Router(config-sbc-sbe-adj-sip)# preferred-transport tcp
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 10.22.160.104
Router(config-sbc-sbe-adj-sip)# statistics method summary
Router(config-sbc-sbe-adj-sip)# signaling-port 5060
Router(config-sbc-sbe-adj-sip)# remote-address ipv4 10.22.160.71 255.255.255.255
Router(config-sbc-sbe-adj-sip)# signaling-peer 10.22.160.71
Router(config-sbc-sbe-adj-sip)# attach
```

Configuring CAC Policy

You need to define call admission control (CAC) policy to instruct the SBC to ignore the media bandwidth fields in the session description protocol (SDP) messages.

Procedure

To define a CAC policy, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)#` **`cac-policy-set`** *`policy-set-id`*	Creates a new CAC policy set for the SBE. The new CAC policy set is empty until you define additional parameters for the policy.
Step 2	`Router(config-sbc-sbe-cacpolicy)#` **`first-cac-table`** *`table-name`*	Defines the first policy table to process when performing the admission control stage of policy.
Step 3	`Router(config-sbc-sbe-cacpolicy)#` **`cac-table`** *`table-name`*	Creates an admission control table for the CAC policy set created in Step 1.
Step 4	`Router(config-sbc-sbe-cacpolicy -cactable)#` **`table-type policy set`**	Configures the CAC table type. Policy set specifies that the event is applied to all entries in the table.
Step 5	`Router(config-sbc-sbe-cacpolicy -cactable)#` **`entry`** *`entry-id`*	Creates an entry in the CAC table.
Step 6	`Router(config-sbc-sbe-cacpolicy -cactable-entry)#` **`media bandwidth-fields ignore`**	Sets the media flag to ignore the media bandwidth fields (b-line) in the session description protocol (SDP) messages. The SBC will use the CODEC value in the SDP message to calculate the baseline bandwidth required for the media stream.
Step 7	`Router(config-sbc-sbe-cacpolicy -cactable-entry)#` **`action cac-complete`**	Configures the action to perform after this entry in the CAC table. The cac-complete keyword specifies that no further action is required for this CAC policy.

	Command	Purpose
Step 8	`Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit`	Exits the CAC table entry configuration mode.
Step 9	`Router(config-sbc-sbe-cacpolicy)# complete`	Marks the end of a CAC policy set definition.
Step 10	`Router(config-sbc-sbe-cacpolicy)# exit`	Exits the CAC policy configuration mode.
Step 11	`Router(config-sbc-sbe)# active-cac-policy-set` *policy-set-id*	Sets the active CAC policy set within the SBE.

The following example shows how to define a call admission control policy for the SBE:

```
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table BW
Router(config-sbc-sbe-cacpolicy)# cac-table BW
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media bandwidth-fields ignore
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy)# complete
Router(config-sbc-sbe-cacpolicy)# exit
Router(config-sbc-sbe)# active-cac-policy-set 1
```

Configuring Call Policies

Create a call policy set to contain the incoming and outgoing route tables. The route tables provide a mapping of each incoming and outgoing call to its corresponding adjacency.

Entries in the SBC route table must match the corresponding entries in the Cisco TelePresence Exchange System routing tables. The carrier ID that you insert on an incoming route (or use as the match parameter on an outgoing route) needs to match the SBC Tag field in the Cisco TelePresence Exchange System. See the "Configuring Routes" section on page 12-1 for information about configuring routes on the Cisco TelePresence Exchange System.

Procedure

To create a call policy set and configure the route tables, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)# call-policy-set` *policy-set-id*	Creates a new policy set for processing calls within the SBE.
Step 2	`Router(config-sbc-sbe-rtgpolicy)# first-call-routing-table` *table-name*	Configures the name of the first routing table for new-call events.
Step 3	`Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table` *table-id*	Creates a new routing table whose entries match the source adjacency.
Step 4	`Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry` *entry-id*	Creates an entry in the routing table.
Step 5	`Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action {complete | {next-table` *go-to-table-name* `} }`	Specifies the next routing table to process if the event matches the entry. Action complete specifies that no further action is required.

	Command	Purpose
Step 6	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# edit-cic replace ds`	Replaces the carrier ID in the SIP message with the specified digit string.
Step 7	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# dst-adjacency target-adjacency`	Configures the destination adjacency for calls that match this table entry.
Step 8	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# match-adjacency key`	Configure the source adjacency as the match value for this table entry.
Step 9	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# exit`	Exits the routing table entry (rtgtable-entry) mode.
Step 10	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# exit`	Exits the routing table (rtgtable) mode.
Step 11	`Router(config-sbc-sbe-rtgpolicy)# rtg-carrier-id-table table-id`	Creates a new routing table whose entries match the carrier ID field.
Step 12	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# entry entry-id`	Creates an entry in the routing table.
Step 13	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# action {complete | {next-table go-to-table-name } }`	Specifies the next routing table to process if the event matches the entry. Action complete specifies that no further action is required.
Step 14	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# edit-cic replace ds`	Replaces the carrier ID in the SIP message with the specified digit string.
Step 15	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# dst-adjacency target-adjacency`	Configures the destination adjacency of an entry in a routing table.
Step 16	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# match-cic key`	Configures the carrier ID match value of the entry.
Step 17	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# exit`	Exits the routing table entry (rtgtable-entry) mode.
Step 18	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# exit`	Exits the routing table (rtgtable) mode.
Step 19	`Router(config-sbc-sbe-rtgpolicy)# complete`	Marks the end of a call policy set definition.
Step 20	`Router(config-sbc-sbe-rtgpolicy)# exit`	Exits the routing policy (rtgpolicy) mode.
Step 21	`Router(config-sbc-sbe)# active-call-policy-set policy-set-id`	Activates the call policy set.

The following example shows how to create a call policy for the SBE and match it to an adjacency:

```
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# first-call-routing-table INCOMING
Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table INCOMING
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-cic replace 200
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency SBC-ACE
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 2
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-cic replace 400
```

```
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency SBC-ACE
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency SBC-UNCM
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 3
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action next-table CIC-OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency SBC-ACE
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 4
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action next-table CIC-OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency SBC-Engine1
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 5
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action next-table CIC-OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency SBC-Engine2
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# exit

Router(config-sbc-sbe-rtgpolicy)# rtg-carrier-id-table OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-cic replace 0
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-cic 200
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 2
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-cic replace 0
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency SBC-UNCM
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-cic 200
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# exit
Router(config-sbc-sbe-rtgpolicy-rtgtable)# exit
Router(config-sbc-sbe-rtgpolicy)# complete
Router(config-sbc-sbe-rtgpolicy)# exit
Router(config-sbc-sbe)# active-call-policy-set 1
```

Configuring SIP Timers

Procedure

To define a SIP timer for call processing within the SBE, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)# sip timer`	Enters the SIP timer configuration mode.
Step 2	`Router(config-sbc-sbe-sip-tmr)# tcp-idle-timeout` *interval*	Specifies the minimum time, in milliseconds, that the TCP connection stays active when it is not processing any traffic. After the timeout period expires, the TCP connection closes. The default value is 120,000 ms.
Step 3	`Router(config-sbc-sbe-sip-tmr)# tcp-connect-timeout` *interval*	Specifies the time, in milliseconds, that the SBC waits for a SIP TCP connection to a remote peer to complete before timing out. The default value is 30,000 ms.
Step 4	`Router(config-sbc-sbe-sip-tmr)# exit`	Exits the SIP timer configuration mode.

The following example shows how to set a SIP timer for the SBE:

```
Router(config-sbc-sbe)# sip timer
Router(config-sbc-sbe-sip-tmr)# tcp-idle-timeout 120000
Router(config-sbc-sbe-sip-tmr)# tcp-connect-timeout 5000
Router(config-sbc-sbe-sip-tmr)# exit
```

Note The values shown in the previous example are the recommended values for the Cisco TelePresence Exchange System configuration.

Defining Blacklists

Procedure

To define a global blacklist for the SBE, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)#` **`blacklist global`**	Creates a global blacklist for configuring event limits.
Step 2	`Router(config-sbc-sbe-blacklist-global)#` **`reason`** *`event`*	Configures the event type for which SBC applies the limit.
Step 3	`Router(config-sbc-sbe-blacklist-global-reason)#` **`timeout`** *`number`* {**`milliseconds`**|**`seconds`**|**`minutes`**|**`hours`**|**`days`**}	Defines the length of time that packets are blocked from the source if the number of authentication requests exceed the set limit.
Step 4	`Router(config-sbc-sbe-blacklist-global-reason)#` **`exit`**	Exits reason configuration mode.
Step 5	`Router(config-sbc-sbe-blacklist-global)#` **`exit`**	Exits blacklist global mode.
Step 6	`Router(config-sbc-sbe)#` **`blacklist global address-default`**	Configures a default event limit for all addresses within the SBE.
Step 7	`Router(config-sbc-sbe-blacklist-global)#` **`reason`** *`event`*	Defines an event type that triggers application of the blacklist.
Step 8	`Router(config-sbc-sbe-blacklist-global-reason)#` **`timeout`** *`number`* {**`milliseconds`**|**`seconds`**|**`minutes`**|**`hours`**|**`days`**}	Defines the length of time that packets are blocked from the source if the number of authentication requests exceeds the set limit.
Step 9	`Router(config-sbc-sbe-blacklist-global)#` **`exit`**	Exits blacklist global mode and completes configuration of default event limits for all addresses.

The follow example shows how to set a global blacklist for the SBE:

```
Router(config-sbc-sbe)# blacklist global
Router(config-sbc-sbe-blacklist-global)# reason authentication-failure
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason bad-address
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason routing-failure
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason endpoint-registration
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason policy-rejection
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason corrupt-message
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global-reason)# exit

Router(config-sbc-sbe)# blacklist global address-default
Router(config-sbc-sbe-blacklist-global)# reason authentication-failure
```

```
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason bad-address
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason routing-failure
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason endpoint-registration
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason policy-rejection
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global)# reason corrupt-message
Router(config-sbc-sbe-blacklist-global-reason)# timeout 1 milliseconds
Router(config-sbc-sbe-blacklist-global-reason)# exit
Router(config-sbc-sbe-blacklist-global)# exit
Router(config-sbc-sbe)#
```

Defining a Media Address

Configure a local media address for traffic that arrives on the SBE for each defined SBC virtual IP address (see the "Creating a Session Border Controller Interface" section on page 20-1). The SBC inserts its own address into the media stream.

After you configure a local media address, the media address cannot be modified while the SBE service is active.

The media address is a pool of IP addresses on the SBE for media relay functionality.

Procedure

To define a media address, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# sbc service-name \`	Enters SBC configuration mode for the specified SBC instance.
Step 2	`Router(config-sbc)# media-address ipv4 IPv4 ip address`	Configures a local media address for traffic that arrives on the DBE. Define one media address for each of the SBC virtual IP addresses.
Step 3	`Router(config-sbc-media-address)# port-range min-port max-port any`	Defines the valid port range for the media address. The optional **any** keyword specifies that the class of service affinity for the port range is any class of service. If the port-range command is not configured, the default *min-port* value is 16384, the default *max-port* value is 32767, and the default class of service affinity is **any**.
Step 4	`Router(config-sbc-media-address)# exit`	Exits the media address configuration mode.
Step 5	`Router(config-sbc)# dbe`	Enters DBE configuration mode.
Step 6	`Router(config-sbc-dbe)# media timeout timeout`	Sets the maximum time in seconds that an SBE waits after receiving the last media packet on a call before cleaning up the call resources.
Step 7	`Router(config-sbc-dbe)# activate`	Activates the DBE.

The following example shows how to define a local media address for each defined SBC virtual IP address:

```
Router(config-sbc)# media-address ipv4 10.22.141.102
Router(config-sbc-media-address)# port-range 16384 32766 any
Router(config-sbc-dbe)# media timeout 600
Router(config-sbc-dbe)# activate
```

CHAPTER 21

Configuring Cisco TelePresence MSE 8000 Series

The following sections describe how to configure the Cisco TelePresence MSE 8000 Series products and the Cisco VCS products:

About the Cisco TelePresence MSE 8000 Series Products

The Cisco TelePresence MSE 8000 Series products support carrier-class telepresence services. The chassis contains a supervisor module and provides nine slots for optional service modules.

The Cisco TelePresence Exchange System uses the following types of service modules:

- Cisco TelePresence MCU MSE 8510—Provides inter-working with single-screen telepresence endpoints that support SIP, H.323, or ISDN standard.
- Cisco TelePresence Server MSE 8710—Provides inter-working with single-screen and multi-screen telepresence endpoints.
- Cisco TelePresence ISDN GW MSE 8321—Provides inter-working with ISDN endpoints.

For additional information, see the Cisco TelePresence MSE 8000 Series website at http://www.cisco.com/en/US/products/ps11340/index.html.

Note When an enterprise wants to deploy Cisco or third-party standards-based (H.323 or ISDN standard) endpoints, the enterprise must install at least one Cisco VCS.

- The required media resources and ISDN gateways used by the Cisco TelePresence Exchange System register directly with the Cisco VCS.
- There are some configuration settings that must be made on the Cisco VCS and SBC that is used within the network. For details, see the "Configuring Call Control" section on page 21-11.
- For additional details on the Cisco VCS, see the Cisco TelePresence Video Communication Server (VCS) website at http://www.cisco.com/en/US/products/ps11337/index.html.

Configuring Cisco TelePresence MSE 8000 Series Settings

The following sections describe how to configure the optional Cisco TelePresence MSE 8000 Series service modules to be used with the Cisco TelePresence Exchange System:

Accessing the Web Interface

After you install the Cisco TelePresence MSE 8000 Series chassis and supervisor module, you can configure the other modules in the chassis by using the supervisor web interface.

Procedure

To access the web interface, do the following procedure:

Step 1 Browse to http://<*IP address of the supervisor module*>.

Step 2 Log in to the system by using a valid administrator username and password.

Step 3 From the navigation pane, choose the **Hardware** tab.

The Blades window is displayed, which lists the available service modules.

Step 4 In the Type column, click the IP address of the applicable service module.

Note You can also configure the service module directly by entering its IP address (as listed under the Port A address column) in a browser window (http://<*IP address of the service module*>). However, there might be a short delay in reporting changes to the supervisor module. Changes made directly from the supervisor module update immediately.

The system displays a summary window for the selected module. Subsequent sections in this chapter provide details about configuring each module.

Configuring SNMP Traps

Procedure

To configure the SNMP traps, do the following procedure:

Step 1 From the navigation pane, choose the **Network** tab.

The supervisor Port A window is displayed.

Step 2 Click the **SNMP** tab.

The SNMP window is displayed.

Step 3 Check the **enable traps** check box, and then enter the IP address of a trap receiver.

Step 4 To save the configuration, click **Update SNMP Settings**.

Configuring Cisco TelePresence Server MSE 8710 Settings

The Cisco TelePresence Server MSE 8710 is a media service module for the Cisco TelePresence MSE 8000 Series platform. The Cisco TelePresence Server MSE 8710 provides conferencing services between Cisco TelePresence and multi-screen standards-based endpoints.

The Cisco TelePresence Server MSE 8710 web interface provides context-sensitive help. Click the information (i) icon in any window to see a description of the fields.

The procedures in this section assume that you browse directly (http://*<IP address of the module>*) to the Cisco TelePresence Server MSE 8710 rather than through the supervisor module. For more details, see the "Accessing the Web Interface" section on page 21-2.

Note Cisco TelePresence Server MSE 8710 modules support master/slave redundancy. Only the master module requires configuration of its parameters. The slave module inherits the configuration from the master.

The following sections describe how to configure the Cisco TelePresence Server MSE 8710:

Configuring Services

Procedure

To configure and enable services, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu.

Step 2 Click the **Services** tab.

The Services window is displayed with the available TCP and UDP services.

Step 3 For Port A, check the check boxes for the following services:

- Web
- Incoming H.323
- Incoming SIP (TCP)
- FTP
- SIP (UDP)

For each service, you can leave the default port number value or you can configure a custom value.

Step 4 If you enabled port B, check the check boxes for the following services:

- Web
- Incoming H.323
- Incoming SIP (TCP)
- FTP
- SIP (UDP)

Step 5 To save the updates, click **Apply changes**.

Configuring H.323 Gatekeeper

Procedure

To configure the H.323 gatekeeper settings, do the following procedure:

Step 1 After logging in, choose **Configuration** from the navigation menu.

Step 2 Click the **System Settings** tab.

The System settings window is displayed.

Step 3 In the H.323 gatekeeper window section, check the **Use gatekeeper** check box, and then enter the IP address of the Cisco TelePresence Video Communication Server in use.

Step 4 In the H.323 ID to register field, enter a registration identifier.

Ensure that you provide a unique identifier for each media server that registers with the same H.323 gatekeeper. Cisco recommends that the registration identifier be 10 digits.

Step 5 To save the updates, click **Apply changes**.

Configuring SIP for Dial-Out Calls

Procedure

To configure the SIP dial-out call settings, do the following procedure:

Step 1 After logging in, choose **Configuration** from the navigation menu.

Step 2 Click the **System Settings** tab.

The System settings window is displayed.

Step 3 From the Outbound call configuration drop-down list, choose **Use trunk**.

Step 4 In the Outbound address field, enter the IP address of the ACE virtual IP (VIP).

Step 5 In the Outbound transport drop-down list, choose **TCP**.

Step 6 To save the configuration, click **Apply changes**.

Configuring API User

Procedure

To configure the API user, do the following procedure:

Step 1 After logging in, choose **Users** from the navigation menu.

The Users window is displayed.

Step 2 Click **Add new user**.

Step 3 In the User ID field, enter **apitest**.

Step 4 To give API administration privileges to the module, check the **Administrator** check box.

Privileges include actions such as adding and deleting conferences.

Step 5 To save the configuration, click **Add user**.

Configuring Cisco TelePresence MCU MSE 8510 Settings

The Cisco TelePresence MCU MSE 8510 is a media service module that provides conferencing service for single-screen H.323 and ISDN standards-based endpoints.

Note The Cisco TelePresence MCU MSE 8510 does not support Cisco TelePresence TIP-based endpoints running CTS Software Release 1.7 or earlier.

The Cisco TelePresence MCU MSE 8510 web interface provides context-sensitive help. Click the information (i) icon in any window to see a description of the fields.

The procedures in this section assume that you browse (http://<*IP address of the module*>) directly to the IP address of the Cisco TelePresence MCU MSE 8510 rather than through the supervisor module. For more details, see the "Accessing the Web Interface" section on page 21-2.

Note Cisco TelePresence Server MCU MSE 8510 modules support master/slave redundancy. Only the master module requires configuration of its parameters. The slave module inherits the configuration from the master.

The following sections describe the configuration tasks:

Configuring Services

Procedure

To configure and enable services, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu (top of window).

The system displays the port A network settings.

Step 2 From the Network window that is displayed, click the **Services** tab.

The Services window is displayed.

Step 3 For port A, check the check boxes for all of the TCP and UDP services except for Tunneled Media.

For each service, you can leave the default port number value or you can configure a custom value.

Step 4 If you have enabled port B, check the check boxes for all of the TCP and UDP services except for Tunneled Media.

Step 5 To save the updates, click **Apply changes**.

Configuring SNMP Traps

Procedure

To configure the SNMP traps, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu.

The system displays the port A network settings.

Step 2 Click the **SNMP** tab.

The system displays the SNMP configuration.

Step 3 Check the **Enable traps** check box, and then enter an IP address for a trap receiver in an available field.

Step 4 To save the updates, click **Update SNMP settings**.

Configuring Conference Settings

Procedure

To configure conference settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

The system displays the conference settings.

Step 2 From the Failed preconfigured participants redial behavior drop-down list, choose **Never redial**.

You do not need to make any additional changes on the **Settings** tab.

Step 3 To save the updates, click **Apply changes**.

Configuring Media Port Settings

Procedure

To configure media port settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **Media ports** tab.

The Media port allocation window is displayed.

Step 3 From the Media port mode drop-down list, choose **HD**.

Step 4 To save the updates, click **Apply changes**.

Configuring H.323 Settings

Procedure

To configure H.323 settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **H.323** tab.

The system displays the H.323 gatekeeper settings.

Step 3 In the H.323 gatekeeper address field, enter the Cisco VCS IP address.

Step 4 In the H.323 ID to register field, enter a registration identifier.

Ensure that you provide a unique identifier for each media server that registers with the same H.323 gatekeeper. Cisco recommends that the registration identifier be 10 digits.

Step 5 To save the updates, click **Apply changes**.

Configuring SIP Dial-Out Call Settings

Procedure

To configure the SIP dial-out call settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **SIP** tab.

The system displays the SIP and SIP call settings.

Step 3 From the SIP registrar usage drop-down list, choose **Disabled**.

Step 4 From the SIP registrar type drop-down list, choose **Standard SIP**.

Step 5 In the Username field, enter a unique number identifier for all dial out calls from the Cisco TelePresence MCU MSE 8510.

Step 6 In the SIP proxy address field, enter the IP address of the ACE virtual IP (VIP).

Step 7 From the Maximum bit rate from Microsoft OCS/LCS clients drop-down menu, choose **<limit disabled>**.

Step 8 At the Outgoing transport option, click the TCP radio button.

Step 9 To save the updates, click **Apply changes**.

Configuring API User

Procedure

To configure the API user, do the following procedure:

Step 1 After logging in, choose **Users** from the navigation menu.

The system displays the configured users window.

Step 2 To add API as a user, click **Add new user**.

Step 3 In the User ID field, enter **apitest**.

Step 4 From the Privilege level drop-down list, choose **administrator** to give API user administration privileges to the module.

Privileges include actions such as adding and deleting conferences.

Step 5 Click **Add user** to save the updates.

Configuring Cisco TelePresence ISDN GW MSE 8321 Settings

The Cisco TelePresence ISDN GW MSE 8321 service module enables the Cisco TelePresence Exchange System to dial out to ISDN endpoints.

The procedures in this section assume that you browse (http://*<IP address of the module>*) directly to the IP address of the Cisco TelePresence ISDN GW MSE 8321 rather than through the supervisor module.

The following sections describe how to configure the ISDN gateway settings:

Configuring Services

Procedure

To configure and enable services, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu (top of window).

The system displays the port A network settings.

Step 2 Click the **Services** tab.

The Services window is displayed, summarizing TCP and UDP services.

Step 3 For Port A, check the check boxes for all of the TCP and UDP services except for Tunneled Media.

For each service, you can leave the default port number value or you can configure a custom value.

Step 4 If you have enabled port B, check the check boxes for all of the TCP and UDP services except for Tunneled Media.

Step 5 To save the updates, click **Apply changes**.

Configuring SNMP Traps

Procedure

To configure the SNMP traps, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu.

The system displays the port A network settings.

Step 2 Click the **SNMP** tab.

The system displays the SNMP configuration.

Step 3 Check the **Enable traps** check box, and then enter an IP address for a trap receiver in an available address field.

Step 4 To save the updates, click **Update SNMP settings**.

Configuring ISDN Settings

Procedure

To configure the ISDN settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **ISDN** tab.

The ISDN window is displayed.

Step 3 In the ISDN codec settings section, check the **H.263** and **H.264** check boxes if they are not already checked.

By default, the system enables all video codecs.

The Content video and Audio codecs allowed fields remain at the default settings.

Step 4 To save the updates, click **Apply changes**.

Configuring ISDN Ports

Procedure

To configure ISDN ports, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **ISDN ports** tab.

The system displays settings for ports 1 through 8. You can use the default setting for most of the fields.

Step 3 In the Directory Number (DN) field, no entry is required.

Step 4 Enter the prefix for national numbers.

For example, in North America, enter 1.

Step 5 Enter the prefix for international numbers.

For example, in North America, enter 011.

Note The above examples only apply to North America. Use appropriate rules for other countries.

Step 6 To save the updates, click **Apply changes**.

Configuring H.323 Settings

Procedure

To configure H.323 settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **H.323** tab.

The system displays the H.323 gatekeeper settings. You can use the default setting for most of the fields.

Step 3 From the H.323 gatekeeper usage drop-down list, choose **Enabled**.

Step 4 In the H.323 gatekeeper address field, enter the IP address of the Cisco VCS.

Step 5 (Optional) If you provision more than one ISDN gateway module, you can use the **Dial plan prefixes** field to select a subset of traffic for each module.

When the start of the dialed digits matches a prefix in the dial plan prefix list, an ISDN call will be scheduled on this gateway.

Step 6 To save the updates, click **Apply changes**.

Configuring IP to ISDN Dial Plan

When configuring the dial plan, note the following:

- By default, the Cisco TelePresence Exchange System applies a prefix of 9 to all numbers. The service provider can change the prefix default during system installation.
- All numbers are defined in an E164 format such as 14085551212.
- At a minimum, a dial plan should remove the prefix of 9, and prepend or append the modified number, as necessary, to allow successful termination on the ISDN network.

Procedure

To configure IP to ISDN dial plan settings, do the following procedure:

Step 1 After logging in, choose **Dial plan** from the navigation menu.

The system displays the IP to ISDN dial plan.

Step 2 To add a rule, click **Add rule**.

The system displays the Add IP to ISDN dial plan rule window.

Step 3 At a minimum, Cisco recommends defining the following rules to recognize numbers that are forwarded from the Cisco TelePresence Exchange System:

a. At the Condition option, click the **Called number matches** radio button, and then enter **9(D*)** in the field next to that option.

b. At the Action option, click the **Call this number** radio button, and then enter **$1** in the field next to that option.

Step 4 Click **Add Rule** to save the configuration.

The system displays the IP to ISDN dial plan window, which displays the new rule.

Step 5 To test the dial plan rules, enter the number in the Number to test field, and then click **Test number**.

Configuring Call Control

The Cisco TelePresence Exchange System provides the capability to communicate with standards-based endpoints by using H.323 signaling. The Cisco VCS acts as an H.323 gatekeeper for the interop endpoints. The Cisco TelePresence Exchange System communicates with the Cisco VCS through an H.323 SBC.

The following sections include information about configuring call control settings on the Cisco VCS and SBC:

- Configuring Cisco VCS Settings, page 21-12
- Configuring H.323 Gateway Settings on the SBC, page 21-12

Configuring Cisco VCS Settings

When an enterprise wants to deploy Cisco TelePresence and third-party standards-based endpoints, the enterprise must install at least one Cisco VCS. The required media resources and ISDN gateways used by the Cisco TelePresence Exchange System register directly with the Cisco VCS.

For dial out calls made from the Cisco TelePresence Exchange System to provisioned endpoints that are registered with a Cisco VCS using a SIP URI, you must add a transform rule (also known as search rule) on the Cisco VCS. This transform rule should replace the IP address of the Cisco VCS with the appropriate domain name in the SIP URI of the provisioned endpoint. The following example shows a transform rule that could be configured on a Cisco VCS. In this example, 1.2.3.4 is the IP address of the Cisco VCS and cisco.com is the domain name in the SIP URI of the provisioned endpoint.

```
Priority  State    Description             Pattern          Type    Behavior   Replace

1         Enabled  Transform IP to Domain  (\w+)@1.2.3.4    Regex   Replace    \1@cisco.com
```

Product information for the Cisco VCS, can be found at http://www.cisco.com/en/US/products/ps11337/index.html.

Configuring H.323 Gateway Settings on the SBC

The Cisco TelePresence Exchange System communicates with the Cisco VCS through an SBC that supports the H.323 protocol.

The required media resources and ISDN gateways used by the Cisco TelePresence Exchange System register directly with the Cisco VCS.

To configure an SBC that supports the H.323 protocol, do the following configuration tasks:

- Configuring Adjacencies with Each Cisco VCS, page 21-12
- Configuring Call Policies, page 21-13

Configuring Adjacencies with Each Cisco VCS

On an SBC that supports the H.323 protocol, configure an adjacency to each Cisco VCS.

Procedure

To configure an adjacency, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)# adjacency (sip | h323) adjacency-name`	Enters configuration mode for the specified SIP or H.323 adjacency. For a Cisco VCS adjacency, enter **h323** as the type of adjacency.
Step 2	`Router(config-sbc-sbe-adj-h323)# signaling-address{ipv4_IP_address|ipv6_IP_address}`	Configures the local IP address of the signaling link to the Cisco VCS.
Step 3	`Router(config-sbc-sbe-adj-h323)# signaling-port port-num [max-port-num]`	Configures the port number for the signaling link to the Cisco VCS.

	Command	Purpose
Step 4	`Router(config-sbc-sbe-adj-h323)#` **`remote-address ipv4`** *`remote-address`*	Configures the IP address of the remote end of the signaling link to the Cisco VCS.
Step 5	`Router(config-sbc-sbe-adj-h323)#` **`signaling-peer`** *`peer-name`*	Configures the H.323 adjacency to use the specified remote signaling-peer. Specify the signaling IPv4 address of the Cisco VCS in dotted-decimal format.
Step 6	`Router(config-sbc-sbe-adj-h323)#` **`signaling-peer-port`** *`peer-name`*	Specify the port number for use with the signaling peer.
Step 7	`Router(config-sbc-sbe-adj-h323)#` **`tech-prefix`** *`prefix-num`*	Specify a prefix number. Calls with this prefix (in the dialed number) are routed to the SBC if the Cisco VCS cannot find any other route for the call.
Step 8	`Router(config-sbc-sbe-adj-h323)#` **`attach`**	Attaches the adjacency to the SBC instance. The adjacency is now available for H.323 call processing.

The following example shows how to create an adjacency between the SBE and a hosted Cisco VCS:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 SBC-VCS
Router(config-sbc-sbe-adj-h323)# signaling-address ipv4 10.22.141.100
Router(config-sbc-sbe-adj-h323)# signaling-port 1719
Router(config-sbc-sbe-adj-h323)# remote-address ipv4 10.22.141.98 255.255.255.255
Router(config-sbc-sbe-adj-h323)# signaling-peer 10.22.141.98
Router(config-sbc-sbe-adj-h323)# signaling-peer-port 1719
Router(config-sbc-sbe-adj-h323)# tech-prefix 1
Router(config-sbc-sbe-adj-h323))# attach
```

The following example shows how to create an adjacency between the SBC and an enterprise Cisco TelePresence Video Communication Server:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 SBC-VCS-ent1
Router(config-sbc-sbe-adj-h323)# signaling-address ipv4 10.22.141.100
Router(config-sbc-sbe-adj-h323)# signaling-port 1719
Router(config-sbc-sbe-adj-h323)# remote-address ipv4 10.22.141.98 255.255.255.255
Router(config-sbc-sbe-adj-h323)# signaling-peer 10.22.141.98
Router(config-sbc-sbe-adj-h323)# signaling-peer-port 1719
Router(config-sbc-sbe-adj-h323))# attach
```

Configuring Call Policies

Procedure

To create a call policy set and configure the route tables, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)#` **`call-policy-set`** *`policy-set-id`*	Creates a new policy set for processing calls within the SBE.
Step 2	`Router(config-sbc-sbe-rtgpolicy)#` **`first-call-routing-table`** *`table-name`*	Configures the name of the first routing table for new-call events.
Step 3	`Router(config-sbc-sbe-rtgpolicy)#` **`rtg-src-adjacency-table`** *`table-id`*	Creates a new routing table whose entries match the source adjacency.

	Command	Purpose
Step 4	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# entry entry-id`	Creates an entry in the routing table.
Step 5	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# match-adjacency key`	Configures the source adjacency as the match value for this table entry.
Step 6	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# action {complete | {next-table go-to-table-name } }`	Specifies the next routing table to process if the event matches the entry. Action complete specifies that no further action is required.
Step 7	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# edit-cic replace ds`	Replaces the carrier ID in the SIP message with the specified digit string.
Step 8	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# exit`	Exits the routing table entry (rtgtable-entry) mode.
Step 9	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# exit`	Exits the routing table (rtgtable) mode.
Step 10	`Router(config-sbc-sbe-rtgpolicy)# rtg-dst-adjacency-table table-id`	Creates a new routing table whose entries match the source adjacency.
Step 11	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# entry entry-id`	Creates an entry in the routing table.
Step 12	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# match-address key`	Configures the carrier ID match value of the entry.
Step 13	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# dst-adjacency target-adjacency`	Configures the destination adjacency of an entry in a routing table.
Step 14	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# action {complete | {next-table go-to-table-name } }`	Specifies the next routing table to process if the event matches the entry. Action complete specifies that no further action is required.
Step 15	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# edit-dst del-prefix ds`	Replaces the carrier ID in the SIP message with the specified digit string.
Step 16	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# dst-adjacency target-adjacency`	Configures the destination adjacency of an entry in a routing table.
Step 17	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# exit`	Exits the routing table entry (rtgtable-entry) mode.
Step 18	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# exit`	Exits the routing table (rtgtable) mode.
Step 19	`Router(config-sbc-sbe-rtgpolicy)# complete`	Marks the end of a call policy set definition.
Step 20	`Router(config-sbc-sbe-rtgpolicy)# exit`	Exits the routing policy (rtgpolicy) mode.
Step 21	`Router(config-sbc-sbe)# active-call-policy-set policy-set-id`	Activates the call policy set.

The following example shows how to create a call policy set and configure route tables:

```
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# first-call-routing-table INCOMING
Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table INCOMING
```

```
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action next-table OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-cic replace 200
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 2
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency SBC-UNCM
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action next-table OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# exit

Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1922 digits
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 2
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1922 digits
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-dst del-prefix 1
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 3
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 139 digits
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# prefix
Router(config-sbc-sbe-rtgpolicy-rtgtable)# exit
Router(config-sbc-sbe-rtgpolicy)# complete
Router(config-sbc-sbe-rtgpolicy)# exit
Router(config-sbc-sbe)# active-call-policy-set 1
```

CHAPTER 22

Configuring Internet Group Management Protocol for IP Multicast Support

The following sections describe how to enable Internet Group Management Protocol (IGMP) snooping and the IGMP querier function on the Cisco Catalyst 6500 Series and Cisco Catalyst 4948 Switches that connect to the Cisco TelePresence Exchange System call engines. In this configuration, IP multicast is used between the two call engines. This chapter also provides IP multicast configuration recommendations for non-Cisco switches.

Multicasting Overview

The Cisco TelePresence Exchange System employs IP multicast to replicate call states between call engine servers in a Cisco TelePresence Exchange System cluster. Therefore, the call engines must be on the same VLAN and subnet.

Note Some of the multicast traffic has a fixed TTL value of 1, which prevents the multicast traffic from being forwarded over multiple layer 3 hops.

Network interface cards (NICs) on end-stations (server or host machine) generally handle multicast traffic. To limit interrupts and congestion on end-stations that do no want to receive multicast traffic, switches can implement IGMP snooping. IGMP snooping allows a switch to learn which end-stations (in this case, the call engines) on the same VLAN want to receive the multicast traffic, and then forward traffic only to those end-station ports that sent IGMP reports and joins for specific groups. The switch then forwards the reports to multicast router (**mrouter**) ports.

By default, IGMP snooping is enabled on all Cisco switches.

IGMP Querier

You must enable the IGMP querier function to support IGMP snooping on a VLAN in which protocol independent multicast (PIM) is not active.

In a network where IP multicast routing is configured, the IP multicast router acts as the IGMP querier. If the IP multicast traffic in a VLAN only needs to be layer 2 switched, an IP multicast router is not required. Without an IP multicast router on the VLAN, you must configure the Cisco Catalyst 6500 Series and Cisco Catalyst 4948 Switches to act as the IGMP querier so that the switch can send queries.

When enabled, the IGMP querier switch sends out periodic IGMPv3 (for the Cisco Catalyst 6500) or IGMPv2 (for the Cisco Catalyst 4948) queries that trigger IGMP report messages from the end-stations (call engines). IGMP snooping listens to these IGMP reports and discovers the multicast groups that each port wishes to receive data. The switch then builds the MAC address table to allow forwarding of the traffic.

Note the following details on the Cisco implementation of the IGMP snooping querier function:

- IGMP querier must be configured on one switch within the VLAN in which the Cisco TelePresence Exchange System call engines operate. However, if the switch fails or disconnects from the VLAN, there might be an outage.
- When IGMP querier is enabled on one switch within the VLAN, it is possible for switches that do not support IGMP querier to operate within that same VLAN.
- IGMP snooping querier supports IGMP version 2 and 3.
- When enabled, the IGMP snooping querier does not start if it detects IGMP traffic from a multicast router.
- When enabled, the IGMP snooping querier starts after 60 seconds with no IGMP traffic detected from a multicast router.
- When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.
- When IGMP snooping is enabled, QoS does not support IGMP packets.

Note The IGMP querier feature is not supported on all switches and all platforms, therefore IGMP querier might not work for all environments. In this case, you can enable the querier function on a Cisco router. For more details, see the "Configuring PIM on a Cisco Router" section on page 22-4.

Configuring the IGMP Querier Functionality on a Cisco Switch

Before You Begin

Ensure that IGMP snooping is enabled on the Cisco Catalyst 6500 Series Switch or Cisco Catalyst 4948 Switch.

Configure a switch within the VLAN with a source address to which the IGMP querier function can forward the queries. The IP address does not need to be the default gateway.

Procedure

To configure the IGMP querier function on a Cisco Catalyst 6500 Series Switch, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# ip igmp snooping`	Globally enables IGMP snooping at the global configuration mode. To disable IGMP snooping, use the **no** form of this command. **Note** By default, IGMP snooping is enabled on all Cisco routers.
Step 2	`Router(config)# interface vlan` *vlan_ID*	Selects the VLAN in which the switch and the call engines operate.
Step 3	`Router(config-if)# ip address` *ip_ address subnet_mask*	Configures the IP address for the switch, which serves as the IGMP querier within the VLAN. The switch must be in the same VLAN in which the call engines operate. When enabled, the IGMP snooping querier uses the switch IP address as the query source address.
Step 4	`Router(config-if)# ip igmp snooping querier`	Enables IGMP querier within the VLAN.
Step 5	`Router(config-if)# end`	Exits interface configuration mode.
Step 6	`Router# show ip igmp interface vlan` *vlan_ID* `| include querier`	Verifies the IGMP querier configuration of the VLAN.

Note IP addresses shown in the configurations are for example purposes only.

The following example defines an IGMP query source address within VLAN 630, and enables and verifies the IGMP querier function on the VLAN:

```
Router# interface vlan 630
Router(config-if)# ip address 10.22.143.241 255.255.255.248
Router(config-if)# igmp snooping querier
Router(config-if)# end
Router# show ip igmp interface vlan 630 | include querier
IGMP snooping fast-leave (for v2) is disabled and querier is enabled
Router#
```

Procedure

To configure the IGMP querier function on a Cisco Catalyst 4948 Switch, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# ip igmp snooping`	Globally enables IGMP snooping at the global configuration mode. To disable IGMP snooping, use the **no** form of this command. **Note** By default, IGMP snooping is enabled on all Cisco routers.
Step 2	`Router(config)# interface vlan` *vlan_ID*	Selects the VLAN in which the switch and the call engines operate.

	Command	Purpose
Step 3	`Router(config-if)# ip address ip_ address subnet_mask`	Configures the IP address for the switch that serves as the IGMP querier within the VLAN. The switch must be in the same VLAN in which the call engines operate.When enabled, the IGMP querier uses the switch IP address as the query source address.
Step 4	`Router(config-if)# exit`	Exits interface configuration mode.
Step 5	`Router(config)# ip igmp snooping querier`	Enables IGMP querier functionality globally on the switch and on all VLANs on the switch.
Step 6	`Router(config)# no ip igmp snooping vlan vlan_ID querier`	Disables IGMP querier on a VLAN. Enter this command for each VLAN for which you want to disable the globally-assigned IGMP querier feature. **Note** Ensure that you do not disable IGMP querier on the VLAN in which the call engines and the switch that serves as the IGMP querier operate.
Step 7	`Router(config)# ip igmp snooping vlan vlan_ID querier address ip_ address`	Specifies the IP address for the switch that serves as the IGMP querier within the VLAN in which the call engine operates.
Step 8	`Router# show ip igmp interface vlan vlan_ID`	Verifies the IGMP querier configuration for the VLAN.

The following example defines an IGMP query source address within VLAN 585, and enables and verifies the IGMP querier function on the VLAN:

```
Router# interface vlan 585
Router(config-if)# ip address 10.22.142.242 255.255.255.224
Router(config-if)# exit
Router(config)# ip igmp snooping querier
Router(config)# no ip igmp snooping vlan 1 querier
Router(config)# ip igmp snooping vlan 585 querier address 10.22.142.242
Router# show ip igmp interface vlan 585
Vlan585 is up, line protocol is up
  Internet address is 10.22.142.242/29
  IGMP is disabled on interface
  Multicast routing is disabled on interface
  Multicast TTL threshold is 0
  No multicast groups joined by this system
  IGMP snooping is globally enabled
  IGMP snooping CGMP-AutoDetect is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping fast-leave (for v2) is disabled
  IGMP snooping querier is enabled. Querier is 10.22.143.241 (this system)
  IGMP snooping explicit-tracking is enabled
  IGMP snooping last member query response interval is 1000 ms
  IGMP snooping report-suppression is enabled
```

Configuring PIM on a Cisco Router

You can configure PIM on Cisco IOS-based routers as well as switches that support layer 3 IP multicast routing (such as the Cisco Catalyst 6500 Series) to allow the router to operate as the IGMP querier, when IGMP querier is not supported on switches within the network.

Note IGMPv2 is the default version for Cisco routers. If IGMPv3 is required in the network, you must specify that version when configuring PIM on the router.

For details on the versions of IGMP support by platform and software version, see the *Cisco Feature Navigator* at http://www.cisco.com/go/fn.

For redundancy, Cisco recommends that you configure two routers with PIM functionality on the VLAN in which the Cisco TelePresence Exchange System call engines operate.

Cisco recommends that you reference the appropriate Cisco router configuration guide on Cisco.com to ensure that all elements of multicasting (such as multicast forwarding, multicast boundaries and rendezvous point, which is only supported on PIM sparse mode) are properly configured for the router.

Before You Begin

Enable IGMP on the switches within the network.

Procedure

To configure PIM on a Cisco router, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# ip multicast-routing`	Globally enables IP multicast routing on the system. **Note** After enabling IP multicast routing on the system, you must configure PIM on the VLAN interface of the call engines. Additionally, disabling IP multicast routing does not remove PIM. PIM must be explicitly removed from the interface configurations.
Step 2	`Router(config)# interface vlan` *vlan_ID*	Selects the VLAN in which the router and the call engine VLAN operate.
Step 3	`Router(config-if)# ip address` *ip_ address subnet_mask*	Configures the IP address of the switch that connects to call engines within the VLAN. When enabled, PIM snooping querier uses the call engine IP address as the query source address.
Step 4	`Router(config-if)# ip pim sparse-mode`	Enables PIM sparse-mode on the VLAN interface.
Step 5	`Router(config-if)# ip igmp version {1|2|3}`	Sets the IGMP version type that the router uses.
Step 6	`Router(config-if)# end`	Exits interface configuration mode.
Step 7	`Router(config)# end`	Exits configuration mode.
Step 8	`Router(config)# show ip pim snooping vlan` *vlan-id* `[neighbor | mac-group | statistics | mroute [`*source-ip* `|` *group-ip*`] ]`	Shows information about a specific VLAN.

The following example enables PIM as an IGMP querier function for a router on the VLAN 630:

```
Router (config)# ip multicast-routing
Router (config)# interface vlan 630
Router(config-if)# ip address 10.22.143.241 255.255.255.248
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip igmp version 3
```

```
Router(config-if)# end
Router(config)# show ip pim snooping vlan 630
3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 10.10.10.4
RP DF Set
```

Configuring IGMP on a Non-Cisco Switch

The Cisco TelePresence Exchange Systems use IGMP version 2 and IGMP version 3 to join (*,G) multicast groups. Membership queries must be sent in order to maintain awareness of active receivers. Active receivers do not normally send IGMP join/reports in an unsolicited fashion; instead, they send a join at application start and when queried (IGMP RFC3376 section 4.1).

The Cisco TelePresence Exchange System call engine servers do not require or support IP multicast over multiple layer 3 hops. Therefore, multicasts occur within the VLAN. All switches that are between or directly connected to call engines must support multicast traffic without the need to see IGMP join/reports. However, because IGMP snooping specifically requires information on IGMP join/reports, a switch or router must act as a IGMP query router.

When you are configuring IGMP on a non-Cisco switch that connects to the Cisco TelePresence Exchange System call engine, note the following configuration guidelines:

- If the switch is multicast-aware and supports IGMP snooping and IGMP querier, do the following tasks:
  - Enable IGMP on the switch if it is not already active.
  - Configure the IGMP querier capability on the switch within the VLAN that the call engines operate.
- If the switch is not multicast-aware and does not support IGMP snooping or other multicast protocol, Cisco recommends placing the call engines in a dedicated VLAN to limit the multicast broadcasts that are addressed to the call engines from being broadcast to other hosts. This ensures that flooded multicast traffic in the broadcast domain will be limited to those hosts that need to receive the multicast traffic.
- If the switch does not support the IGMP querier function, but does support disabling IGMP snooping, then disable IGMP snooping on the switch.

  When you disable IGMP snooping, the multicast traffic is flooded to all hosts in the VLAN. For this reason, Cisco recommends placing the call engines in a dedicated VLAN in order to limit the multicast flooding to those hosts that need to receive the multicast traffic.
- If the switch does not support the IGMP querier function, and does not allow disabling of IGMP snooping, then configure a router interface in the call engine VLAN with PIM sparse-mode.

  Additionally, configure the router to block forwarding of multicast traffic over layer 3 hops.

CHAPTER 23

Configuring Cisco Jabber Support

Revised July 19, 2012

The procedures in this chapter address the minimum configuration requirements necessary on the Cisco Unified Communications Manager (Unified CM) and Cisco TelePresence Video Communication Server (VCS) to support the following Cisco Jabber clients:

Cisco Jabber for Windows in Unified CM Mode

The procedures in this section assume that the Cisco Unified Communications Manager (Unified CM), Cisco Unified Presence Server (CUPS), and Cisco Jabber for Windows are already installed and active in the network. For minimum software requirements for the Unified CM, CUPS, and Cisco Jabber for Windows, see the applicable *Release Notes for the Cisco TelePresence Exchange System*, at http://www.cisco.com/go/ctx-relnotes.

The procedures in this section address the following minimum configuration requirements necessary on the Unified CM for Cisco Jabber for Windows support.

- Create a SIP profile. This profile will be associated with the Cisco Jabber devices.
- Configure region settings to allow users to place a video call.
- Configure device settings to enable video capabilities on the Cisco Jabber devices.

Product information for the Unified CM, can be found at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

The Cisco TelePresence Exchange System does not require any specific configuration settings on the CUPS. Product information for the CUPS can be found at http://www.cisco.com/en/US/products/ps6837/index.html

Product information for Cisco Jabber for Windows can be found at http://www.cisco.com/en/US/products/ps12511/index.html

This section includes the following topics:

- Configuring Device Settings in Unified CM, page 23-4

Logging into the Unified CM Administration Application

Procedure

To log into the Unified CM Administration application, do the following procedure:

Step 1 Access a web browser that is supported by the Unified CM Administration application from any user PC in your network. In the address bar of the web browser, enter the following URL:

`https://Unifed_CM-server-name`

where *Unified_CM-server-name* is the name or IP address of the server.

Note If your network uses DNS services, you can specify the hostname of the server where the Unified CM is installed. If your network does not use DNS services, you must specify the IP address of the server.

Step 2 Log in with your assigned administrative privileges.

Step 3 From the Navigation field at the upper right corner of the page, click **Cisco Unified Communications Manager Administration**, and then click **Go**.

The system returns to the Cisco Unified Communications Manager Administration home page.

Creating a SIP Profile

Procedure

To create a SIP profile, do the following procedure:

Step 1 Click **Device**. Under **Device Settings**, click **SIP Profile**.

Step 2 Click **Add New** at the bottom of the page or click the **+** sign at the top of the page.

Step 3 Enter the settings as indicated in Table 23-1 to configure the SIP profile. Leave default settings for fields not included in Table 23-1.

Step 4 To save your changes, click **Save** at the bottom of the page.

Step 5 Apply the SIP profile to the Cisco Jabber for Windows devices. For instructions, see the applicable *Cisco Unified Communications Manager Administration Guide* for your release, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Table 23-1 SIP Profile Settings for Cisco Jabber for Windows

Field	Setting
Reroute Incoming Request to new Trunk based on	Choose **Never**.
RSVP Over SIP	Choose **Local RSVP**.
Fall Back to Local RSVP	Check the check box.
SIP Rel1XX Options	Choose **Disabled**.
Deliver Conference Bridge Identifier	Uncheck the check box.
Early Offer support for voice and video calls (insert MTP if needed)	Uncheck the check box.
Send send-receive SDP in mid-call INVITE	Uncheck the check box.
Allow Presentation Sharing using BFCP	Check the check box.

Configuring Region Settings in Unified CM

If you are using multiple Unified CM regions, you must configure the audio and video bit rate for high definition calls for each region. The procedure in this section assumes that the following regions are already configured on the Unified CM.

- Region of the CSF client (Cisco Jabber for Windows)
- Region of the desk phone
- Region of the SIP trunk for the Cisco TelePresence Exchange System SBC

Procedure

To configure the audio and video bit rate for a region, do the following procedure:

Step 1 Click **System** > **Region**.

Step 2 Click **Find**.

Step 3 Select a region.

Step 4 Enter the settings as indicated in Table 23-2 to configure the audio and video bit rate for the region. Leave default settings for fields not included in Table 23-2.

Step 5 To save your changes, click **Save** at the bottom of the page.

Step 6 Associate the region to the Cisco Jabber for Windows devices. For instructions, see the applicable *Cisco Unified Communications Manager Administration Guide* for your release, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Table 23-2 SIP Profile Settings for Cisco Jabber for Windows

Field	Setting
Region	Default
Max Audio Bit Rate	256 kbps (L16, AAC-LD)

Table 23-2 SIP Profile Settings for Cisco Jabber for Windows (continued)

Field	Setting
Max Video Call Bit Rate (Includes Audio)	32000
Link Loss Type	Use System Default.

Configuring Device Settings in Unified CM

The procedure in this section assumes that the Cisco Jabber for Windows devices are already configured in the Unified CM.

Procedure

To configure device settings to enable video capabilities on the Cisco Jabber devices, do the following procedure:

Step 1 Click **Device** > **Phone**.

Step 2 Click **Find**

Step 3 Select a phone.

Step 4 Under the "Product Specific Configuration Layout" section, set the **Video Capabilities** field to **Enabled**. Leave default settings for all other fields.

Step 5 To save your changes, click **Save** at the bottom of the page.

Cisco Jabber for iPad in Unified CM Mode

The procedures in this section assume that the Cisco Unified Communications Manager (Unified CM), Cisco Unified Presence Server (CUPS), and Cisco Jabber for iPad are already installed and active in the network. For minimum software requirements for the Unified CM, CUPS, and Cisco Jabber for iPad, see the applicable *Release Notes for the Cisco TelePresence Exchange System*, at http://www.cisco.com/go/ctx-relnotes.

The procedures in this section address the following minimum configuration requirements necessary on the Unified CM for Cisco Jabber for iPad support.

- Create a SIP profile. This profile will be associated with the Cisco Jabber devices.
- Configure region settings to allow users to place a video call.
- Configure device settings to enable video capabilities on the Cisco Jabber devices.

Product information for the Unified CM, can be found at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

The Cisco TelePresence Exchange System does not require any specific configuration settings on the CUPS. Product information for the CUPS can be found at http://www.cisco.com/en/US/products/ps6837/index.html

Product information for Cisco Jabber for iPad can be found at http://www.cisco.com/en/US/products/ps12430/index.html

This section includes the following topics:

Logging into the Unified CM Administration Application

Procedure

To log into the Unified CM Administration application, do the following procedure:

Step 1 Access a web browser that is supported by the Unified CM Administration application from any user PC in your network. In the address bar of the web browser, enter the following URL:

`https://Unifed_CM-server-name`

where *Unified_CM-server-name* is the name or IP address of the server.

Note If your network uses DNS services, you can specify the hostname of the server where the Unified CM is installed. If your network does not use DNS services, you must specify the IP address of the server.

Step 2 Log in with your assigned administrative privileges.

Step 3 From the Navigation field at the upper right corner of the page, click **Cisco Unified Communications Manager Administration**, and then click **Go**.

The system returns to the Cisco Unified Communications Manager Administration home page.

Creating a SIP Profile

Procedure

To create a SIP profile, do the following procedure:

Step 1 Click **Device**. Under **Device Settings**, click **SIP Profile**.

Step 2 Click **Add New** at the bottom of the page or click the **+** sign at the top of the page.

Step 3 Enter the settings as indicated in Table 23-3 to configure the SIP profile. Leave default settings for fields not included in Table 23-3.

Step 4 To save your changes, click **Save** at the bottom of the page.

Step 5 Apply the SIP profile to the Cisco Jabber for iPad devices. For instructions, see the applicable *Cisco Unified Communications Manager Administration Guide* for your release, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Table 23-3 SIP Profile Settings for Cisco Jabber for IPad

Field	Setting
Reroute Incoming Request to new Trunk based on	Choose **Never**.
RSVP Over SIP	Choose **Local RSVP**.
Fall Back to Local RSVP	Check the check box.
SIP Rel1XX Options	Choose **Disabled**.
Deliver Conference Bridge Identifier	Uncheck the check box.
Early Offer support for voice and video calls (insert MTP if needed)	Uncheck the check box.
Send send-receive SDP in mid-call INVITE	Uncheck the check box.
Allow Presentation Sharing using BFCP	Check the check box.

Configuring Region Settings in Unified CM

If you are using multiple Unified CM regions, you must configure the audio and video bit rate for high definition calls for each region. The procedure in this section assumes that the following regions are already configured on the Unified CM.

- Region of the CSF client (Cisco Jabber for iPad)
- Region of the SIP trunk for the Cisco TelePresence Exchange System SBC

Procedure

To configure the audio and video bit rate for a region, do the following procedure:

Step 1 Click **System** > **Region**.

Step 2 Click **Find**.

Step 3 Select a region.

Step 4 Enter the settings as indicated in Table 23-4 to configure the audio and video bit rate for the region. Leave default settings for fields not included in Table 23-4.

Step 5 To save your changes, click **Save** at the bottom of the page.

Step 6 Associate the region to the Cisco Jabber for iPad devices. For instructions, see the applicable *Cisco Unified Communications Manager Administration Guide* for your release, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Table 23-4 Region Settings for Cisco Jabber for iPad

Field	Setting
Region	Default
Max Audio Bit Rate	256 kbps (L16, AAC-LD)

Table 23-4 Region Settings for Cisco Jabber for iPad (continued)

Field	Setting
Max Video Call Bit Rate (Includes Audio)	32000
Link Loss Type	Use System Default.

Configuring Device Settings in Unified CM

The procedure in this section assumes that the Cisco Jabber for iPad devices are already configured in the Unified CM.

Procedure

To configure device settings to enable video capabilities on the Cisco Jabber devices, do the following procedure:

Step 1 Click **Device** > **Phone**.

Step 2 Click **Find**

Step 3 Select a phone.

Step 4 Under the "Product Specific Configuration Layout" section, set the **Video Capabilities** field to **Enabled**. Leave default settings for all other fields.

Step 5 To save your changes, click **Save** at the bottom of the page.

Cisco Jabber Video for TelePresence Enterprise for iPad in VCS Mode

The procedures in this section assume that the Cisco TelePresence Video Communication Server (VCS) and Cisco Jabber Video for TelePresence Enterprise (formerly known as Movi) for Mac OS X are already installed and active in the network. For minimum software requirements for the Cisco VCS and Jabber Video, see the applicable *Release Notes for the Cisco TelePresence Exchange System*, at http://www.cisco.com/go/ctx-relnotes.

The procedures in this section address the following minimum configuration requirements necessary on the Cisco VCS for Cisco Jabber for iPad in VCS mode support:

- Create a SIP zone.
- Create search rules to allow calls from Jabber Video endpoints to reach the Cisco TelePresence Exchange System.

Product information for the Cisco VCS, can be found at http://www.cisco.com/en/US/products/ps11337/index.html.

Product information for Cisco Jabber Video for TelePresence can be found at http://www.cisco.com/en/US/partner/products/ps11328/tsd_products_support_series_home.html

This section includes the following topics:

Logging into the Cisco VCS

Procedure

To log into the Cisco VCS application, do the following procedure:

Step 1 Access a web browser that is supported by the Cisco VCS Administration application from any user PC in your network. In the address bar of the web browser, enter the following URL:

```
https://VCS-server-name
```

where *VCS-server-name* is the name or IP address of the server.

Note If your network uses DNS services, you can specify the hostname of the server where the Cisco VCS is installed. If your network does not use DNS services, you must specify the IP address of the server.

Step 2 Log in with your assigned administrative privileges.

Step 3 From the Navigation field at the upper right corner of the page, click **Cisco Unified Communications Manager Administration**, and then click **Go**.

The system returns to the Cisco VCS login home page.

Creating a Zone

You must configure a SIP zone for communication between the Cisco VCS and Cisco TelePresence Exchange System SBC.

Procedure

To create a new zone, do the following procedure:

Step 1 On the Create search rule page, choose **VCS configuration** > **Zones** > **New**

Step 2 Create a new zone with the settings as indicated in Table 23-5.

Step 3 To save your configuration, click **Save**.

Step 4 Verify that the peer 1 IP address is active. If the address is not active, an error message will appear to the right of the Peer 1 address field. If the address is active, the following string will appear in green text:

SIP: Active: *<IP address of Cisco TelePresence Exchange System SBC>:<port>*

For example, if the IP address of the Cisco TelePresence Exchange System SBC is 10.22.139.103 and the port number is 5060, the string would appear as follows:

```
SIP: Active: 10.22.139.103:5060
```

Table 23-5 New Zone Settings

Field	Setting
Name	CTX SBC
Hop Count	15
H323 Mode	Off
SIP Mode	On
Port	5060
Transport	TCP
Accept proxied registrations	Allow
Authentication policy	Do not check credentials.
SIP authentication trust mode	Off
Peer 1 address	Enter the IP address of the Cisco TelePresence Exchange System SBC.
Zone profile	Default

Creating Search Rules

Based on your Cisco TelePresence Exchange System call routing configuration, you must configure search rules (also known as transform rules) for Meet-Me and Rendezvous meeting dial in calls and for direct dial calls. These search rules allow calls from Jabber Video endpoints (as well as other H.323 or SIP endpoints) to reach the Cisco TelePresence Exchange System.

Procedure

To create search rules for direct dial calls and dial in calls that use a service number, do the following procedure:

Step 1 On the Create search rule page, choose **VCS configuration > Dial plan > Search rules > New**

Step 2 Create a new search rule for each of the following conditions:

- Dial in calls that use a service number. (see Table 23-6)
- Dial in calls that use a service number and conference ID (see Table 23-7)
- Direct dial calls (see Table 23-8)

Step 3 To save your configuration, click **Save**.

Table 23-6 Search Rule Settings for Dial In Service Number

Field	Setting
Rule name	Dial in service number
Description	Transform SIP URI alias (username@domain) to a string value
Priority	40

Table 23-6 Search Rule Settings for Dial In Service Number (continued)

Field	Setting
Source	Any
Request must be	No authenticated
Mode	Alias pattern match
Pattern type	Regex
Pattern string	(<*service number*>)\@.* For example, if the service number configured in the Cisco TelePresence Exchange System is 14085550100, enter the pattern string as follows: `(14085550100)\@.*`
Pattern behavior	Replace
Replace string	\1@<*IP address of Cisco TelePresence Exchange System SBC*> For example, if the IP address of the Cisco TelePresence Exchange System SBC is 10.22.139.103, enter the string as follows: `\1@10.22.139.103`
On successful match	Stop
Target zone	CTX SBC zone created in the "Creating a Zone" section on page 23-8
State	Enabled

Table 23-7 Search Rule Settings for Service Number with Conference ID

Field	Setting
Rule name	Dial in service number including 8-digit Cisco TelePresence Exchange System conference ID
Description	Dial in call using Cisco TelePresence Exchange System conference ID
Priority	40
Source	Any
Request must be	No authenticated
Mode	Alias pattern match
Pattern type	Regex

Table 23-7 Search Rule Settings for Service Number with Conference ID (continued)

Field	Setting
Pattern string	(<*service number*>**(\d{8}))\@.* For example, if the service number configured in the Cisco TelePresence Exchange System is 14085550100, enter the pattern string as follows: `(14085550100\*\*(\d{8}))\@.*`
Pattern behavior	Replace
Replace string	\1@<*IP address of Cisco TelePresence Exchange System SBC*> For example, if the IP address of the Cisco TelePresence Exchange System SBC is 10.22.139.103, enter the string as follows: `\1@10.22.139.103`
On successful match	Stop
Target zone	CTX SBC zone created in the "Creating a Zone" section on page 23-8
State	Enabled

Table 23-8 Search Rule Settings for Direct Dial Calls

Field	Setting
Rule name	Direct dial
Description	Direct dial call
Priority	50
Source	Any
Request must be	No authenticated
Mode	Alias pattern match
Pattern type	Regex
Pattern string	(\d{11})\@.*
Pattern behavior	Replace
Replace string	\1@<*IP address of Cisco TelePresence Exchange System SBC*> For example, if the IP address of the Cisco TelePresence Exchange System SBC is 10.22.139.103, enter the string as follows: `\1@10.22.139.103`
On successful match	Stop
Target zone	CTX SBC zone created in the "Creating a Zone" section on page 23-8
State	Enabled

PART 5

Maintaining the Cisco TelePresence Exchange System

CHAPTER 24

Managing Database Backups

The Database Backup window allows the administrator to view scheduled database backups that are configured on the Cisco TelePresence Exchange System and to view past database backups and database restores.

Additionally, you can initiate a manual, on-demand backup of an existing scheduled backup, and restore a database backup on the database server of the system.

The following sections describe viewing the current backup schedule, and viewing past database backup and database restores information as part of database server maintenance:

Viewing the Scheduled Database Backup

The currently configured backup schedule for the database backup is found at the top of the Database Backup window (System > Database Backup) and is displayed as Current Backup Schedule. An example of the display is as follows:

Current Backup Schedule: Daily at 2:08 PM America/Los_Angeles

For details on configuring scheduled database backups, see the "Configuring Database Backups" section on page 8-7.

Viewing Past Database Server Backups and Restores

You can view details for past database server backups and backup restores.

Details of database backups include the following:

- Start time of the backup
- Duration of the backup
- IP address or name of the backup server
- Filename of the backup file
- Type of backup (such as scheduled)

- Status of the backup (such as success)
- Log of the backup

Details of database restores include the following:

- Date of the backup file that is restored on the database server
- Start time of the backup
- IP address or name of the backup server
- Filename of the backup file
- Type of backup (such as on demand)
- Status of the backup (such as success)
- Log of the backup

Before You Begin

Configure scheduled backups for the Cisco TelePresence Exchange System database server.

Procedure

To view existing scheduled backups for the database server, do the following procedure:

Step 1 From the navigation pane, choose **System > Database Backup**.

The Database Backup window is displayed.

Note When a database backup schedule is configured for the system, the schedule is displayed to the right of the Current Backup Schedule heading (such as **Daily at 2:08 PM America/Los_Angeles**).

Step 2 To view details for a past database backup or database restore, do one of the following:

- To view details for a past database backup, click an entry in the Start Time column in the Past Backups section of the Database Backup window.
  - To display the latest backup at the top of the listing, click the sorting icon (triangle) that is next to the Start Time heading so that it points downward.
  - To display the earliest backup, click the sorting icon that is next to the Start Time heading so that it points upward.
- To view details for a past database restore, click an entry in the Backup Restores column in the Past Restores section of the Database Backup window.
  - To display the latest database restore at the top of the listing, click the sorting icon (triangle) that is next to the Start Time heading so that it points downward.
  - To display the earliest database restore at the top of the listing, click the sorting icon (triangle) that is next to the Start Time heading so that it points upward.

Step 3 (Optional) To filter on the number of backup or restore entries that display in the window, do one of the following:

- To view the number of database backups for a specific period, click the **T** icon next to the Start Time column heading in the Past Backup section, enter the starting and ending dates in the filter panel that appears, and then click **Filter**.

- To view the number of database restores for a specific period, click the **T** icon next to Backup From column heading, enter the starting and ending dates in the filter panel that appears, and then click **Filter**.

Note (Optional) The system can also filter on the following parameters: duration of the backup, server IP address, backup filename, size of the database file, backup type, and status. To define a filter (in all cases), click the **T** icon next to the name of the column heading (such as Status), enter the appropriate information in the filter panel that appears, and then click **Filter**.

Caution When you click **Clear Filter** within the Past Backups and Past Restores sections of the Database Backup window, the system clears all user-defined filters for that section.

Step 4 (Optional) To clear a specific filter, click the **T** icon next to the appropriate column heading (such as Filename), and then click **Clear** in the filter panel that appears.

Performing a Manual Database Backup

Before You Begin

Configure scheduled backups for the Cisco TelePresence Exchange System database server.

Procedure

To do a manual (on-demand) database backup on the database server, do the following procedure:

Step 1 From the navigation pane, choose **System > Database Backup**.

The Database Backup window is displayed.

Step 2 To start a manual backup, click **Start a Manual Backup**.

Note To cancel a database backup that is in process, click **Cancel Currently Running Backup** when the database backup begins.

When the backup is complete, an entry for the backup is displayed on the Past Backups listing. The result of the backup is displayed under the Status column and the type of backup is displayed as ON_DEMAND under the Type column.

To ensure that the latest backup is displayed at the top of the Past Backups listing, click the sorting icon (triangle) next to the Start Time heading so that it points downward.

Restoring a Database Server Backup

Before You Begin

Caution Do not perform the restore process while the system is in service. Verify that no meetings are active on the system during the restore process, or all previous meeting configuration details will be lost.

- Configure scheduled backups for the Cisco TelePresence Exchange System database server.
- Configure a retention policy for the database server backups to ensure that an adequate number of backups are available.
- Verify that the Cisco TelePresence Server MSE 8710 (TPS) resource is online.
- Do not log in to the TPS or Cisco TelePresence MCU MSE 8510 (MSE 8510) administrative console. We recommend that you do not delete the conference names manually. Otherwise, perform the following functions:
  - Reprovision the TPS or MSE 8510 resource.
  - Set the TPS or MSE 8510 resource to a maintenance state.
  - Modify the Conference Name and Vendor Config fields. Then, save your changes.
- For all other media resources and the Cisco TelePresence Manager resource, verify that the user credentials and conference names have not been modified between database server backups and backup restores. If you made modifications, verify that you updated the appropriate media resource.
- After you installed the latest software version or reverted back to the previous software version, wait at least 10 minutes before you start the restore process.

  If the restore process fails to restart the call engine servers, gracefully start each call engine server by using the **utils service sipserver start** command. For detailed information about this command, see the Appendix C, “Command Reference”.

Procedure

To restore a database backup on the database server, do the following procedure:

Step 1 From the navigation pane, choose **System > Database Backup**.

The Database Backup window is displayed.

Step 2 To view available database backups to restore on the database server, scroll down to the Past Restores section.

Step 3 To restore a database backup, click **Restore a Backup** (near the top of the page).

The Restore a Backup window is displayed.

Step 4 To select a specific backup to restore onto the database server, click the radio button next to the entry listed in the Completed Time column.

Step 5 To restore the backup, click **Restore**.

The Confirm Restore panel appears.

Step 6 To confirm and start backup restore, click **Start Restore**.

Note To cancel the backup restore, click **Cancel** in the Confirm Restore panel.

The system immediately logs the administrator out of the administration console.

Note The administrator does not have access to the administration console until the system restores the database backup file on the database server and the restoration process is complete (approximately five minutes).

Step 7 To ensure that the restore was successful, log back in to the administration console.

Step 8 From the navigation pane, choose **System > Database Backup**.

Step 9 Under the Status column in the Past Restores section of the Database Backup window, ensure that the state for the latest backup restore is displayed as Success.

To display the latest database restore at the top of the listing, click the sorting icon (triangle) that is next to the Start Time heading so that it points downward.

CHAPTER 25

Meeting Diagnostics

This chapter describes how to use configuration events and meeting events to view details on meetings and to diagnose Cisco TelePresence Exchange System configuration issues; it includes the following sections:

Viewing an Audit Trail

An audit trail displays recent configuration changes; the database server saves the last 30 days of configuration changes.

You can filter the list of configuration events based on:

- Name—describes the configuration item type
- Description—describes the change that was made to the item type
- Agent—indicates the user ID of the user who made the change (by default, guest)
- Events—indicates the type of modification: insert (new configuration), update, or delete
- Time—allows sorting of events for a specific date or range of dates

Procedure

To view the audit trail, do the following procedure:

Step 1 From the navigation pane, choose **Diagnostics > Audit Trail**.

The Audit Trail window is displayed.

Step 2 (Optional) To create a filter, click the **T** next to the appropriate column heading (name, agent, event, or time).

Step 3 In the filter panel that is displayed, do one of the following:

- For name and event filters, check the check box next to those items that you want to filter.
- For agent and time filters, enter the variable that you want to filter within the field.

Step 4 To save the filter, click **Filter**.

You can clear a filter definition by clicking **Clear**.

Step 5 (Optional) To clear all configured filters on the Diagnostics > Audit Trail window, click **Clear Filters**.

All filters are reset to their defaults.

Step 6 (Optional) To order the list of events, do one of the following:

- To display the latest event at the top of the listing, click the sorting icon (triangle) that is next to the Time heading so that it points downward.
- To display the earliest event at the top of the listing, click the sorting icon (triangle) that is next to the Time heading so that it points upward.

Starting a Log Collection Session

The log collection displays all the new and previous archives for all the administration and call engine servers that are in the cluster.

Before You Begin

- Only system administrators, administrators, and service desk users can start and stop a log collection session.
- Provisioning and read-only users are not allowed to start and stop a log collection session.
- All user roles can view and download the log archive tar files.
- The log archives will reside locally on your system.

You can filter the list of logs based on:

- File Name—indicates the filename of the log archive
- Start Time—indicates the start time from the latest or earliest log archive
- End Time—indicates the end time from the latest or earliest log archive
- File Size—indicates the size of the log archive

To start a log collection session for the appropriate servers, do the following procedure:

Step 1 From the navigation pane, choose **Diagnostics > Log Capture**.

The Log Capture window displays.

Step 2 To specify the duration of the log capture, check the **Stop capturing logs** check box.

Step 3 In the after field, enter **the time duration** in increments for how long that you want the system to collect the logs.

By clicking the **up** or **down** arrows, you can also increase or decrease the time duration in increments of 5. The default value is 60 minutes. The range is from 5 to 300 minutes.

Step 4 To start capturing the logs, click **Start Capturing**.

While the log collection is in progress, the red flashing dot displays.

Step 5 To stop the log collection, click **Stop Capturing**.

Each row displays the new or previous captured log tar file.

Step 6 To download the appropriate tar file, click **the provided link**.

The tar file is downloaded to your designated location. It contains the requested log archives for the specified time period.

Step 7 (Optional) To clear all configured filters on the Diagnostics > Log Capture window, click **Clear Filters**.

All filters are reset to their defaults.

Step 8 (Optional) To order the list of log archives, do one of the following:

- To display the latest log archive at the top of the listing, click the sorting icon (triangle) that is next to the Start Time and End Time heading so that it points downward.
- To display the earliest log archive at the top of the listing, click the sorting icon (triangle) that is next to the Start Time and End Time heading so that it points upward.

Viewing the Reservation Pool Usage

Available only to system administrators and administrators, the reservation pool usage displays the number of ports or segments that are reserved for a given resource pool, and displays the time buckets. All Meet-Me pools (also called *scheduled*) display the start and end times in 15-minute interval time buckets. Because Rendezvous pools (also called *timeless*) are not limited to a start time, the reservation information is displayed in a single time bucket. For each resource type, this window also displays the maximum number of single-screen and three-screen endpoints that can be reserved for the specified time period.

If you specify the start time and duration of the meeting, the View Reservation Pool Usage window displays all of the Meet-Me pools within that time period and the Rendezvous pools. If you check the Rendezvous Meeting check box, this window displays all of the future Meet-Me pools and the Rendezvous pools.

To view the reservation pool usage for a meeting, do the following procedure:

Procedure

Step 1 From the navigation pane, choose **Diagnostics > Reservation Pool Usage**.

The Reservation Pool Usage Parameters window displays.

Step 2 Choose the appropriate service provider from the drop-down list.

Step 3 Choose the appropriate region from the drop-down list.

Step 4 Choose the appropriate reservation type from the drop-down list.

Step 5 (Optional) To display the Rendezvous pools, check the Rendezvous **Meeting** check box.

Step 6 (Optional) To display the interval time buckets for the Meet-Me pools, follow these steps:

a. Click the **calendar** icon to enter a date for the meeting. An interactive calendar displays.

b. Choose the **date** on the calendar.

Tip You can choose a different month or year by clicking the < and > arrows.

c. In the time fields, enter the **start time of the meeting**.

d. Choose the time zone in which the given reservation pool is located from the drop-down list.

Step 7 In the Duration in Minutes field, enter **the duration of the meeting** in 15-minute intervals.

Note This field is optional only if you checked the Rendezvous Meeting check box.

Step 8 (Optional) To enable the reservation pool for a large meeting, check the **Large Meeting** check box.

Step 9 Click **Submit**.

The View Reservation Pool Usage window displays. For information about the field descriptions, see Table 25-1.

Step 10 (Optional) To clear all configured filters on the Scheduled Pool Usage table or Rendezvous Pool Usage table, click **Clear Filters**.

All filters are reset to their defaults.

Related Topics

- Reservation Pool Usage Fields, page 25-4

Reservation Pool Usage Fields

Table 25-1 Reservation Pool Usage Fields

Field	Description
Scheduled Pool Usage	
Resource Kind	A list of the available media resource groups for the Meet-Me pools. You can check the check box next to the resources that you want to filter; then, click **Filter**.
Bucket Start Time	Start time for the applicable resource in 15-minute interval time buckets. You can enter the bucket start date or time; then, click **Filter**.
Bucket End Time	End time for the applicable resource in 15-minute interval time buckets. You can enter the bucket end date or time; then, click **Filter**.
Max Capacity	The maximum number of segments that can participate concurrently for the applicable Meet-Me pool. You can enter the variable in the field; then, click **Filter**. By default, this field displays all entries as they are filtered by the parameters entered in the Reservation Pool Usage Parameters window.
Reserved Capacity	Reserved capacity, in segments, which was reserved for the applicable Meet-Me pool. You can enter the variable in the field; then, click **Filter**.
Rendezvous Pool Usage	
Resource Kind	A list of the available media resource groups for the Rendezvous pools. You can check the check box next to the resources that you want to filter; then, click **Filter**.

Table 25-1 Reservation Pool Usage Fields (continued)

Field	Description
Max Capacity	The maximum number of segments that can participate concurrently for the applicable Rendezvous pool. You can enter the variable in the field; then, click **Filter**. By default, this field displays all entries as they are filtered by the parameters entered in the Reservation Pool Usage Parameters window.
Reserved Capacity	Reserved capacity, in segments, which was reserved for the applicable Rendezvous pool. You can enter the variable in the field; then, click **Filter**.
Remaining Capacity	
Resource Kind	Type of media resource.
Remaining Capacity	Number of segments that are still available.
Max1-screen Endpoints	The maximum number of single-screen endpoints that can be reserved on this type of media resource by using the specified parameters.
Max3-screen Endpoints	The maximum number of three-screen endpoints that can be reserved on this type of media resource by using the specified parameters.

Related Topics

- Viewing the Reservation Pool Usage, page 25-3

Viewing Allocation Pool Usage

Available only to system administrators and administrators, the allocation pool usage displays the allocated ports or segments for a given resource pool and resource group.

You can filter the list of pool allocations based on:

- Service Provider—indicates the service provider
- Region—indicates the region of the media bridge resource
- Reservation Type—indicates whether the system provided a guaranteed or best-effort level of service
- Resource Group—indicates the media bridge resources that are associated with the group
- Resource Kind—indicates the media bridge resource for the Meet-Me pool or Rendezvous pool
- Is Large—indicates whether the resource pool is allocated for large meetings or not
- Total Capacity—indicates the total port capacity
- Allocated Capacity—indicates the allocated media bridge resource capacity
- Remaining Capacity—indicates the number of segments that are still available

Procedure

To view the allocation pool usage, do the following procedure:

Step 1 From the navigation pane, choose **Diagnostics > Allocation Pool Usage**.

The View Allocation Pool Usage window displays.

Step 2 (Optional) To create a filter, click the **T** next to the appropriate column heading (service provider, region, reservation type, resource group, resource kind, is large, total capacity, allocated capacity, or remaining capacity).

Step 3 In the filter panel that is displayed, do one of the following:

- For resource kind and is large filters, check the check box next to those items that you want to filter.
- For service provider, region, reservation type, resource group, total capacity, allocated capacity, and remaining filters, enter the variable that you want to filter within the field.

Step 4 To save the filter, click **Filter**.

You can clear a filter definition by clicking **Cancel**.

Step 5 (Optional) To clear all configured filters on the on the View Allocation Pool Usage window, click **Clear Filters**.

All filters are reset to their defaults.

Viewing Meeting Diagnostics

Detailed meeting diagnostics are available for meetings that you schedule in the Cisco TelePresence Exchange System.

There are two Meeting Diagnostic views:

- Participants View—Summarizes the participants that are currently (and previously) involved in the meeting; the resources involved in the meeting (such as the Cisco TelePresence Multipoint Switch, the Cisco TelePresence Server MSE 8710, and the Cisco TelePresence MCU MSE 8510); and the reserved and available capacity for each resource.

  For active meeting diagnostics, this view also allows you to mute, unmute, drop, redial, and send text messages to display to specified participants. See the "Field Reference for the Participants View of Active Meeting Diagnostics" section on page 13-35.

- Events View—Provides a chronological summary of all events that occur from the time a meeting is scheduled to the time the meeting is completed.

  The Cisco TelePresence Exchange System retains meeting diagnostics events for up to 30 days from the time the event occurred. The system automatically purges events that exceed this 30-day limit. If the total number of events retained by the system reaches 100,000, the system retains only the most recent 100,000 events and automatically purges the rest.

  For active meeting diagnostics, see the "Field Reference for the Events View of Active Meeting Diagnostics" section on page 13-37.

For a detailed description of the Lock Meeting or Unlock Meeting options in the Active Meeting Control area, see the "Managing Active Meetings" section on page 13-32.

For instructions on viewing meeting diagnostics, see the "Procedure" section on page 25-7. For instructions on viewing meeting diagnostics for active meetings, see the "Viewing Meeting Diagnostics for Active Meetings" section on page 25-7.

Available only to dial-out participants, you can also use the Diagnostics tool to reconnect participants who have been disconnected from meetings. For instructions, see the "Reconnecting Disconnected Meeting Participants to a Meeting" section on page 25-10.

Procedure

To view meeting diagnostics for a meeting, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 2 Click the applicable meeting to go to the Meeting Details page.

Note If the meeting that you selected is currently an active meeting, the Meeting Diagnostics page for active meetings displays.

Step 3 From the toolbar, click **Go to Diagnostics**.

The Meeting Diagnostics page is displayed.

Related Topics

- Field Reference for the Participants View of Meeting Diagnostics Fields, page 25-8
- Field Reference for the Events View of Meeting Diagnostics, page 25-9

Viewing Meeting Diagnostics for Active Meetings

Active meeting participants can also view the diagnostic details.

The meeting event diagnostic information in the Events View displays only the event state (changes) of the meeting. However, the resource event diagnostic information in the Events View displays when the system allocates or deallocates the resources for that meeting. Based on whether a meeting has active participants or not, the system can change the state of the meeting. Therefore, multiple events that display the same state can be generated during the duration of the meeting.

To view meeting diagnostics for active meetings, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Active Meetings**.

The page lists only currently active meetings and automatically refreshes as meetings become active and inactive.

Step 2 To view the meeting diagnostics for a specific active meeting, click the **subject of the meeting** link.

The Meeting Diagnostics page is displayed.

Related Topics

- Managing Active Meetings, page 13-32
- Field Reference for the Participants View of Active Meeting Diagnostics, page 13-35
- Field Reference for the Events View of Active Meeting Diagnostics, page 13-37

Field Reference for the Participants View of Meeting Diagnostics Fields

Table 25-2 Field Reference for the Participants View of Meeting Diagnostics Fields

Field	Description
Resources	
Resource	A link to the management site of the resource. You can click the resource to view the details.
Host	The IP address (or hostname, if you enable DNS) of the resource.
Region	A text string indicating the region of the resource.
Reserved Capacity	The number of segments reserved by Cisco TelePresence Exchange System on the resource for this meeting.
Available Capacity	The number of segments available for the meeting.
Static Meeting ID	The static meeting ID that is being used by the resource for the current meeting.
Participants Joining or Currently in the Meeting	
Participant	The access number of the participant.
Endpoint Name	Cisco TelePresence Exchange System-provisioned name of the endpoint. You can click the name to view the endpoint details. The following values may also be displayed: • Guest Endpoint—Dial-out guest endpoint. • Unprovisioned Endpoint—Dial-in unprovisioned endpoint.
Join Time	Time and date stamp indicating when the participant joined the meeting.
Capacity Used	Number of media bridge resource segments that are utilized by the participant.
Dial-In/Dial-Out	Text string indicating whether the participant is a dial-in or dial-out call.
Mute Status	Whether the participant is currently muted or unmuted.
Details	A link to a page that provides additional details.
Previous Participants	
Participant	The access number of the participant.
Endpoint Name	Cisco TelePresence Exchange System-provisioned name of the endpoint. You can click the name to view the endpoint details. The following values may also be displayed: • Guest Endpoint—Dial-out guest endpoint. • Unprovisioned Endpoint—Dial-in unprovisioned endpoint.
Join Time	Time and date stamp indicating when the participant joined the meeting.

Table 25-2 Field Reference for the Participants View of Meeting Diagnostics Fields (continued)

Field	Description
Leave Time	Time and date stamp indicating when the participant was disconnected from the meeting.
CDR	A link to the call detail record.
Details	A link to a page that provides additional details.
Redial	To use this option, first check the check box for one or more participants that are not in the meeting. Then, click **Redial**. A new entry displays in the Participants Joining or Currently in the Meeting table. However, the entries for this table are not affected. When you attempt to redial, the status in the Dial-In/Dial-Out field changes to Requesting Dialout and then to Dialing out. After the disconnected participant is reconnected, the status changes to Dial-Out. The redial option is available only for dial-out participants. **Note** When the meeting has ended, the Redial button is no longer available.

Related Topics

- Field Reference for the Participants View of Active Meeting Diagnostics, page 13-35
- Viewing Meeting Diagnostics, page 25-6
- Field Reference for the Events View of Meeting Diagnostics, page 25-9

Field Reference for the Events View of Meeting Diagnostics

Table 25-3 Field Reference for the Events View of Meeting Diagnostics

Field	Description
Meeting Events	
Time	Chronological list of time and date stamps associated with meeting events.
Description	Text descriptions detailing each event that occurs, for example: • Meeting Ended • Meeting Started • Meeting Resources Reserved • Participant Joined • Participant Left
Details	A link to a page that provides additional details.
Alarms Near Meeting Time	
Severity	Text description and icon indicating whether the alarm signifies an error or is providing information only.
Time	Time and date stamp indicating when the alarm was generated.

Table 25-3 Field Reference for the Events View of Meeting Diagnostics (continued)

Field	Description
Summary	Text description of the alarm.
Server	Name of the server on which the alarm occurred.

Related Topics

- Field Reference for the Events View of Active Meeting Diagnostics, page 13-37
- Viewing Meeting Diagnostics, page 25-6
- Field Reference for the Participants View of Meeting Diagnostics Fields, page 25-8

Reconnecting Disconnected Meeting Participants to a Meeting

When a participant has been disconnected from a meeting for any reason, help-desk personnel can reconnect the participant to the meeting, by using the diagnostic tool.

Note The redial option is available only for dial-out endpoints that were originally added at the time of scheduling a meeting or modifying an active meeting. For more information about active meetings, see the "Managing Active Meetings" section on page 13-32.

Disconnected participants are shown in the Participants View of the diagnostic tool. When the redial button is clicked, the participant is reconnected to the meeting.

Note The redial button is not visible to admins with the Read-Only user role.

Procedure

To reconnect disconnected participants to a meeting, do the following procedure:

Step 1 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 2 Click the applicable meeting to go to the Meeting Details page.

Step 3 From the toolbar, click **Go to Diagnostics**.

The Meeting Diagnostics page is displayed.

Step 4 In the Previous Participants table, check the check box of each participant that you want to reconnect. Then, click **Redial** (located at the bottom of the table).

The system dials out to the endpoint, and gives the endpoint three opportunities to pick up. The participant reappears in the current participants table before the endpoint picks up. Reconnecting a disconnected participant may take up to 30 seconds.

Note If the meeting in question occurred in the past, participants listed in the Previous Participants table cannot be reconnected to the meeting; thus, the Redial button is no longer available.

Step 5 To return to the Meetings page, from the toolbar, click **Meeting Details Page**.

CHAPTER 26

Configuring SNMP

Configuring SNMP is optional for the Cisco TelePresence Exchange System. At minimum, however, Cisco recommends that you configure SNMP on the administration servers to monitor the entire system via the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB. This product-specific MIB enables you to monitor all nodes in the Cisco TelePresence Exchange System server cluster as well as all resources that you configure on the Cisco TelePresence Exchange System. With this product-specific MIB, the remote management system needs to monitor or query only one of the administration servers to determine the status of each resource and cluster node.

If you also want to monitor the hardware and operating system (such as the server memory, CPU, disk usage, power supplies, and fans) of each server, configure SNMP on all nodes in the Cisco TelePresence Exchange System server cluster.

Note Cisco recommends that SNMP clients use a 5-second or longer timeout when querying the Cisco TelePresence Exchange System.

This chapter includes the following sections:

Restrictions for SNMP

- SNMP version 1 is not supported. Only SNMP versions 2c and 3 are supported.
- SNMP inform requests are not supported. SNMP notifications are sent as traps only.
- SNMP configurations are not replicated between servers. Whenever you change the SNMP configuration, whether via the CLI or via SNMP Set operations to read-write objects, you must manually apply the same configuration changes to each of the other servers.
- The CISCO-SYSLOG-MIB is implemented and will respond to queries, but the syslog messages are currently unformatted and raw.

- The Cisco TelePresence Exchange System supports MIB persistence on indexes and read-write objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB. The system automatically saves the indexes and read-write set operations every four hours, starting at midnight (0000) UTC.
  - If you set an object, then wait four hours before restarting the SNMP service or rebooting the server. Otherwise, the object may be set to its previous value after the SNMP service restart.
  - If you configure an SNMP-monitored item (such as a media resource) via the Cisco TelePresence Exchange System administration console, CLI, or API, then wait four hours before restarting the SNMP service or rebooting the server. Otherwise, the item you added may not remain indexed as it was before the SNMP service restart.
  - Indexes are not reused. If you configure an SNMP-monitored item and then remove it, the index for that item will be void. If you add the item back again, the item will get a new index.

For additional details about the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, see the "CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB" section on page D-1.

Supported MIBs

The CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB was created specifically to manage the Cisco TelePresence Exchange System. This MIB is implemented only on the administration servers, but it manages all six nodes in the server cluster and monitors all resources that are configured on the Cisco TelePresence Exchange System.

Other RFC-based MIBs are also supported and may be implemented on all Cisco TelePresence Exchange System servers to provide hardware and operating system information, for example, about the CPU, memory, power supplies, and fans. IBM servers implement the IBM MIBs.

For a complete list of supported MIBs, see the *MIBs Supported by Cisco TelePresence Exchange System* document at ftp://ftp.cisco.com/pub/mibs/supportlists/CTXSystem/CTXSystem-supportlist.htm.

Related Topics

- CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, page D-1
- Resource Monitoring, page 26-3

About SNMP on the Cisco TelePresence Exchange System

See the following sections:

- Cluster Node Monitoring, page 26-3
- Resource Monitoring, page 26-3
- Trap Flood Mitigation, page 26-3

Cluster Node Monitoring

Each administration server independently queries each node in the Cisco TelePresence Exchange System server on a 30-second interval by running one of the following commands, depending on the node role:

- utils service adminserver status
- utils service database status
- utils service sipserver status

The status returned from each query is updated in the ctxClusterNodeTable, and you can view the status as the operational state in the System > Cluster Nodes area of the administration console.

Resource Monitoring

The Cisco TelePresence Exchange System monitors the resources that are configured in the system on a fixed interval. Table 26-1 shows how and when each resource type is monitored.

Note The system does not monitor the following resources:

- Any resources that are configured to be in the maintenance state in the Cisco TelePresence Exchange System.
- Resources that are not configured in the Cisco TelePresence Exchange System, such as the Cisco TelePresence Video Communication Server.

Table 26-1 Resource Monitoring Intervals and Methods

Resource Type	Resource Examples	Probe Interval	Probe Methods
SIP-based resources	• Cisco Session Border Controller • Cisco TelePresence Multipoint Switch • Cisco router with IVR[1] • Cisco TelePresence ISDN GW MSE 8321	15 seconds	SIP OPTIONS PING
XML-RPC–based resources	• Cisco TelePresence Server 7010 • Cisco TelePresence MCU MSE 8510	15 seconds	SIP OPTIONS PING and XML-RPC PING
Cisco TelePresence Manager		5 seconds	API PING

1. IVR = Integrated Voice Response

Trap Flood Mitigation

As a rate-limiting feature, traps are sent at 5-second intervals. Specifically, instead of generating and sending a trap as soon as each event is received, the system collects events for up to 5 seconds and then generates traps on the fifth second.

Most of the traps are stateful, meaning that they have an *inAlarm* trap and a *clearing* trap. Using a stateful trap ensures that additional events for the same issue are not sent more than once, unless the trap was cleared first.

How to Configure SNMP

Which tasks you must complete, and on which servers you complete those tasks, depend on the extent of your SNMP implementation.

To	Do This
(Strongly recommended) Use the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB to obtain Cisco TelePresence Exchange System–specific information about the entire server cluster and configured resources.	Complete these tasks on both administration servers: • Adding SNMP Users, page 26-4 • Adding SNMP Trap Destinations, page 26-6 • Adding a Cluster-Identifying VIP Address to SNMP Notifications, page 26-8 • Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, page 26-10
(Recommended) Monitor the server-specific hardware and operating system, such as the memory, CPU, disk usage, power supplies, and fans.	Complete these tasks on all six Cisco TelePresence Exchange System servers: • Adding SNMP Users, page 26-4 • Adding SNMP Trap Destinations, page 26-6
Remove SNMP configurations.	• Deleting an SNMP User, page 26-5 • Removing an SNMP Trap Destination, page 26-7 • Removing the Cluster-Identifying VIP Address from SNMP Notifications, page 26-10
Troubleshoot SNMP issues.	• Troubleshooting SNMP, page 26-12

Adding SNMP Users

Complete this procedure on each Cisco TelePresence Exchange System server on which you want to enable SNMP queries.

Before You Begin

- For each server on which you complete this task, make sure that you use the exact same configuration on the other server of the same node role.
- You can add up to ten SNMP users on each server.
- For details about any command or its options, see Appendix C, "Command Reference."
- If you are not sure whether to complete this task, or on which server to complete it, see the "How to Configure SNMP" section on page 26-4.

Procedure

Step 1 Log in to the CLI of the server.

Step 2 Enter one of the following commands, depending on whether you use SNMP version 3 or version 2c:

- **set snmp user add 3** *username* {**r** | **w** | **rw**} [**authNoPriv** | **authPriv** | **authNoPriv**] *passphrase*
- **set snmp user add 2c** *community-string* {**r** | **w** | **rw**}

Note If you use both SNMP versions 3 and 2c, make sure that no version 3 usernames are the same as any version 2c community strings.

Examples:

```
admin: set snmp user add 3 mrtg rw authNoPriv tstpwd
Successfully added user
admin: set snmp user add 2c public r
Successfully added user
```

Step 3 To verify the SNMP user addition, enter the **show snmp users** command.

```
admin: show snmp users
1)  Username: mrtg                      Version: v3
       Level: AuthNoPriv                   Mode: RW

2) Community: public                    Version: v2c
       Level: n/a                          Mode: R
```

You should also now be able to query the Cisco TelePresence Exchange System server on which you added the SNMP user.

Step 4 Repeat this procedure on the other applicable nodes in the Cisco TelePresence Exchange System server cluster.

What to Do Next

Proceed to the "Adding SNMP Trap Destinations" section on page 26-6.

Deleting an SNMP User

Before You Begin

For details about any command or its options, see Appendix C, "Command Reference."

Procedure

Step 1 Log in to the CLI of the server.

Step 2 To display the configured SNMP users, enter **show snmp users**.

```
admin: show snmp users
1)  Username: mrtg                      Version: v3
       Level: AuthNoPriv                   Mode: RW

2) Community: public                    Version: v2c
       Level: n/a                          Mode: R
```

```
3)  Username: testuser                  Version: v3
       Level: AuthNoPriv                   Mode: RW
```

Step 3 Enter one of the following commands, depending on whether you use SNMP version 3 or version 2c:

- **set snmp user del 3** *username*
- **set snmp user del 2c** *community-string*

Example:

```
admin: set snmp user del 3 testuser
Successfully deleted user
```

Step 4 To verify the SNMP user deletion, enter the **show snmp users** command.

```
admin: show snmp users
1)  Username: mrtg                      Version: v3
       Level: AuthNoPriv                   Mode: RW

2) Community: public                    Version: v2c
       Level: n/a                          Mode: R
```

Adding SNMP Trap Destinations

Complete this procedure on each Cisco TelePresence Exchange System server from which you want to receive trap notifications.

Before You Begin

- For each server on which you complete this task, make sure that you use the exact same configuration on the other server of the same node role.
- You can add up to five trap destinations on each server.
- For details about any command or its options, see Appendix C, "Command Reference."
- If you are not sure whether to complete this task, or on which server to complete it, see the "How to Configure SNMP" section on page 26-4.

Procedure

Step 1 Log in to the CLI of the server.

Step 2 Enter one of the following commands, depending on whether you use SNMP version 3 or version 2c:

- **set snmp trapdest add 3** *username destination*[**:***port*] [*level*] *passphrase* [*engineID*]
- **set snmp trapdest add 2c** *community-string destination*[**:***port*] [*passphrase*]

The *destination* is the IP address or hostname of the host where you want the Cisco TelePresence Exchange System to send trap notifications.

For the *level*, specify **authNoPriv**, **authPriv**, or **noauthNoPriv**.

Step 3 To verify the trap destination addition, enter the **show snmp trapdests** command.

```
admin: show snmp trapdests
  1) Host = 192.0.2.162 (Version 2c)
```

```
   Version 2c Options:
      Community = public
```

Step 4 Repeat this procedure on the other applicable nodes in the Cisco TelePresence Exchange System server cluster.

What to Do Next

If you want to identify redundant product-specific notifications from the same Cisco TelePresence Exchange System server cluster, proceed to the "Adding a Cluster-Identifying VIP Address to SNMP Notifications" section on page 26-8.

Removing an SNMP Trap Destination

Procedure

Step 1 Log in to the CLI of the server.

Step 2 Enter **set snmp trapdest del**.

```
admin: set snmp trapdest del
  1) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = TimTrap               PW   = authpriv
           Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  2) Host = 10.101.180.49 (Version 3)

     Version 3 Options:
            User = TimTrap2              PW   = authpriv
           Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  3) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = trapusr               PW   = trappass
           Level = authnopriv            Hash = md5
        EngineID = 0x8000DEECAFE8111BEEFADE
```

Step 3 When prompted, enter the number from the displayed list to specify the trap destination to delete.

```
  Enter which trap number to delete: 2
Successfully deleted trap destination
```

Step 4 Enter the **show snmp trapdests** command and verify that the deleted trap destination no longer appears.

```
admin: show snmp trapdests
  1) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = TimTrap               PW   = authpriv
           Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  2) Host = 10.101.180.49:162 (Version 3)
```

```
Version 3 Options:
       User = trapusr               PW   = trappass
      Level = authnopriv            Hash = md5
   EngineID = 0x8000DEECAFE8111BEEFADE
```

Adding a Cluster-Identifying VIP Address to SNMP Notifications

Product-specific notifications about the Cisco TelePresence Exchange System are sent from the two administration servers via the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB. Because both of the administration servers are active, the system may send redundant SNMP notifications.

To help you identify redundant product-specific notifications from the same Cisco TelePresence Exchange System server cluster, you can configure the administration servers to add an SNMP object called "SNMP-COMMUNITY-MIB::snmpTrapAddress" to the VarBind list of each trap that is generated by the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB.

The snmpTrapAddress value specifies a virtual IP (VIP) address that your remote management system can associate with a specific Cisco TelePresence Exchange System server cluster. You can configure one of the following VIP addresses as the snmpTrapAddress value:

- (Recommended) VIP address of the call engine servers as configured on the SIP load balancer, which is the Cisco Application Control Engine (ACE).
- SNMP (UDP port 161) VIP address that you configure on the ACE to enable it to act as a load-balanced reverse proxy to the administration servers. Specifically, configure an SNMP server farm on the ACE as a reverse proxy where one administration server is a real server (rserver), while the second administration server is a standby rserver.

  If you choose this option, all SNMP Get and Set operations to the administration server SNMP VIP address will go only to the administration server that you configured as the rserver. If the rserver goes down, the Get and Set operations will go only to the administration server that you configured as the standby rserver.

  Note Cisco does not recommend using this SNMP VIP address to monitor the hardware and operating system for the administration servers. If you do so, you will monitor only one of the two administration servers for the cluster. To monitor the hardware or operating system of any Cisco TelePresence Exchange System server, Cisco recommends that you use the IP address of the specific server.

- VIP address to identify both administration servers in the cluster. This VIP address is not required for installation and is not configured anywhere else on the Cisco TelePresence Exchange System.

When two product-specific notifications include the same snmpTrapAddress value, then you know that they were sent from the same Cisco TelePresence Exchange System server cluster. The source IP address of each trap packet identifies the administration server that sent the notification.

Note In each SNMP trap that is sent by any node in the Cisco TelePresence Exchange System server cluster, the source IP address identifies which node sent the trap. If you complete the procedure below, the SNMP-COMMUNITY-MIB::snmpTrapAddress object will be added only to notifications from the administration servers that are generated by the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB.

Before You Begin

- If you complete this task, make sure that you use the exact same configuration on both administration servers in the cluster.
- Complete the procedure in the "Adding SNMP Trap Destinations" section on page 26-6.
- Import the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB into your network management server or SNMP monitoring package.

  To download the MIB, go to:
  ftp://ftp.cisco.com/pub/mibs/v2/CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB.my

Procedure

Step 1 Log in to the CLI of the administration server.

Step 2 Enter **set adminserver trapvip ena** *vip-address*, specifying the VIP address to use as the snmpTrapAddress value that your remote management system can associate with the Cisco TelePresence Exchange System server cluster:

```
admin: set adminserver trapvip ena 10.22.128.212
Updated SNMP Trap VIP to 10.22.128.212
```

Step 3 To verify the configuration, enter **show trapvip**.

```
admin: show trapvip
SNMP Trap VIP: 10.22.128.212
```

Step 4 Repeat this procedure for the second administration server in the cluster.

Examples

The following example shows a received trap *without* the snmpTrapAddress VarBind:

```
TRAP: UDP: [10.21.79.129]:60482 (. 0.0)
    sysUpTimeInstance = Timeticks: (45688631) 5 days, 6:54:46.31
    snmpTrapOID.0 = OID: ciscoCTXSysSystemBackupStatusChg
    ctxSystemBackupStatus.0 = INTEGER: normal(1)
    ctxNotifyMessage.2 = STRING: 2010-10-28T02:49:10.021Z Backup Status OK Cause:
StartTime:2010-10-18T00:00:00.000Z
```

The following example shows a received trap *with* the snmpTrapAddress VarBind:

```
TRAP: UDP: [10.21.79.129]:60482 (. 0.0)
    sysUpTimeInstance = Timeticks: (45688631) 5 days, 6:54:46.31
    snmpTrapOID.0 = OID: ciscoCTXSysSystemBackupStatusChg
    snmpTrapAddress.0 = IpAddress: 10.22.128.212
    ctxSystemBackupStatus.0 = INTEGER: normal(1)
    ctxNotifyMessage.2 = STRING: 2010-10-28T02:49:10.021Z Backup Status OK Cause:
StartTime:2010-10-18T00:00:00.000Z
```

What to Do Next

(Optional) If you want to disable any of the traps that are sent by the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, proceed to the "Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB" section on page 26-10.

Removing the Cluster-Identifying VIP Address from SNMP Notifications

Before You Begin

If you complete this task, make sure that you do so on both administration servers in the cluster.

Procedure

Step 1 Log in to the CLI of the administration server.

Step 2 Enter **set adminserver trapvip dis**.

```
admin: set adminserver trapvip dis
Disabled SNMP Trap VIP
```

Step 3 To verify the configuration, enter **show trapvip**.

```
admin: show trapvip
SNMP Trap VIP is not enabled/configured on this server.
```

Step 4 Repeat this procedure for the second administration server in the cluster.

Related Topics

- Adding a Cluster-Identifying VIP Address to SNMP Notifications, page 26-8

Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB

To control whether or not the system sends specific notifications that are offered by the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, you can use SNMP Set operations on the objects under the ctxNotifyConfigObjects subtree.

Note

- The SNMP user must have read-write access to use SNMP Set operations.
- SNMP configurations are not replicated between Cisco TelePresence Exchange System servers. If you change the value of any read-write objects on one administration server, you must manually implement the same change on the other administration server.

For objects that are set to true, the notifications that are controlled by those objects will be enabled. For objects that are set to false, the notifications that are controlled by those objects will be disabled.

Use SNMP Get operations to check the values of these objects.

The CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB offers the following notifications:

- ciscoCTXSysAdminServersStatusChg
- ciscoCTXSysDatabaseServersStatusChg
- ciscoCTXSysCallEnginesStatusChg
- ciscoCTXSysResourceStatusChg
- ciscoCTXSysSystemConfigStatusChg

- ciscoCTXSysSystemBackupStatusChg
- ciscoCTXSysLicenseFailure
- ciscoCTXSysUserAuthFailure
- ciscoCTXSysClusterNodeDown
- ciscoCTXSysClusterNodeUp
- ciscoCTXSysResourceDown
- ciscoCTXSysResourceUp
- ciscoCTXSysResourceAllocFailure
- ciscoCTXSysCallSetupFailure
- ciscoCTXSysCallAbnormalDisconnect
- ciscoCTXSysErrorHistoryEvent

Example

Suppose that you do not want the system to send ciscoCTXSysUserAuthFailure notifications. Open the MIB file and find the notification description, which states which object in the ctxNotifyConfigObjects subtree controls whether or not the notification is sent:

```
ciscoCTXSysUserAuthFailure NOTIFICATION-TYPE
    OBJECTS         { ctxNotifyMessage }
    STATUS          current
    DESCRIPTION
        "This notification will be sent when a user authentication
        failure results in CTX System.
           1. User authentication errors while trying to log into
              the CTX System Admin UI.
           2. User authentication errors while trying to log into
              the CTX System CLI.

        ctxAuthFailureNotifyEnable controls whether this notification
        is sent or not."
   ::= { ciscoTelepresenceExchangeSystemMIBNotifs 8 }
```

In the MIB file, find the object description, which includes the following information:

- Which notifications the object controls—an object may control more than one notification.
- Default value of the object—true (notifications are enabled) or false (notifications are disabled).

For example:

```
ctxAuthFailureNotifyEnable OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object specifies if the authentication failure traps
        should be enabled or disabled. Setting this to TRUE
        will enable the notifications.  Setting this to FALSE
        will disable the notifications.

        The default setting for authentication failures is
        FALSE/disabled in order to prevent unnecessary event
        flooding.

        This object controls the generation of the following
        notifications:
```

```
        ciscoCTXSysUserAuthFailure"
DEFVAL          { false }
::= { ctxNotifyConfigObjects 3 }
```

Using your preferred method and tools, use SNMP Get operations to view the current value of the ctxAuthFailureNotifyEnable object in the ctxNotifyConfigObjects subtree.

If you want to change the value, use SNMP Set operations to do so on both administration servers.

Related Topics

- CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, page D-1
- Restrictions for SNMP, page 26-1

Troubleshooting SNMP

- You can use the **utils snmp get** and **utils snmp walk** commands to troubleshoot SNMP from within the Cisco TelePresence Exchange System.
- If a product-specific notification is not being sent as expected, see the "Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB" section on page 26-10.

CHAPTER 27

Configuring Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and to discover the platform of those devices. CDP is media- and protocol-independent, and it runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches. By using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN.

Use of SNMP with the CDP Management Information Base (MIB) allows network management applications to learn the device type and the SNMP agent address of neighboring devices, and to send SNMP queries to those devices. Cisco Discovery Protocol uses the CISCO-CDP-MIB.

Each device that is configured for CDP sends periodic "hello" messages, known as advertisements, to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or hold-time, information to indicate the length of time a receiving device should hold the CDP information before discarding it. Each device also listens to the periodic CDP messages that are sent by others in order to learn about neighboring devices, and to determine when their interfaces to the media go up or down.

This chapter includes the following sections:

Configuring CDP

By default, CDP is enabled on the Bond 0 interface of each Cisco TelePresence Exchange System server.

Before You Begin

- CDP configurations are not replicated between servers. When you change the CDP configuration, you must manually apply the same configuration changes to each of the other servers.
- To see the current CDP configuration, see the "Displaying the CDP Configuration" section on page 27-2.

Procedure

Step 1 Log in to the CLI of the server.

Step 2 To see which interfaces are available for you to enable CDP, enter **show cdp list**.

```
admin: show cdp list
```

```
Available Interfaces:
   bond0
   bond1
```

Step 3 To enable or disable CDP on one or all interfaces, enter the following command:

set cdp {**enable** | **disable**} {*interface* | **all**}

To specify an *interface*, enter one of the values in the CLI output from when you completed Step 2.

Step 4 To set the frequency of CDP advertisements, enter the following command:

set cdp timer *seconds*

Step 5 To set the advertised amount of time that a receiving device should hold the information that is sent by this device before discarding it, enter the following command:

set cdp holdtime *seconds*

Step 6 To verify the configuration, proceed to the "Displaying the CDP Configuration" section on page 27-2.

Related Topics

- Command Reference, page C-1

Displaying the CDP Configuration

Procedure

Step 1 Log in to the CLI of the server.

Step 2 To see the current CDP configuration, enter **show cdp config**.

```
admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 60 seconds
    Hold Time   : 180 seconds
    Enabled on  : bond0
```

Related Topics

- Command Reference, page C-1

CHAPTER 28

Changing the Network Configurations

Typically, the Cisco TelePresence Exchange System network configurations are completed only during installation. If, however, you need to make changes to the network configurations after installation, see the following topics:

Changing the IP Address of an Administration or Call Engine Server

Typically, the IP addresses of the administration server and call engine server are configured only during installation of the servers. Nevertheless, you may complete this task to change or correct the configuration after installation, for example, if you move the servers into a different network.

Before You Begin

- Completing this task causes loss of connectivity to the server and involves restarting the server. Cisco recommends that you complete this task only during a maintenance period.
- Access the CLI via the console to avoid losing administrator connectivity to the server.

Procedure

Step 1 Log in to the CLI of the server.

Step 2 Disable the bond between Ethernet 0 and Ethernet 1 by entering the **set network failover dis** command.

```
admin: set network failover dis
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?
```

Step 3 Enter **yes** to confirm that you want to continue with disabling the bond.

```
Enter "yes" to continue or any other key to abort:
```

```
yes
executing ...
```

Step 4 Change the IP address by entering the following command:

set network ip eth0 *IP-address subnet-mask*

Example:

```
admin: set network ip eth0 10.22.139.106 255.255.255.240
          ***   W A R N I N G   ***
The system will be rebooted after the change.
```

Step 5 When prompted, enter **y** to confirm that you want to continue with changing the IP address.

```
Continue (y/n)? y
SIP server listening address has been changed to 10.22.139.106
Please restart the SIP server using the 'utils service sipserver stop|start' command for
the change to take effect


Warning: Restart could take up to 5 minutes...
Shutting down Service Manager will take some time..
\   Service Manager shutting down services... Please Wait
DONE!!!!

Broadcast message from root (Thu Feb 17 23:58:48 2011):

The system is going down for reboot NOW!

Restart has succeeded
```

Step 6 Log back in to the CLI of the server.

Step 7 If you changed the VLAN of the server, also complete the following steps:

a. Change the default gateway by entering the following command:

set network gateway *IP-address*

Example:

```
admin: set network gateway 10.22.139.97
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity.
```

b. When prompted, enter **y** to confirm that you want to continue with changing the default gateway.

```
Continue (y/n)? y
```

Step 8 Re-enable the bond between Ethernet 0 and Ethernet 1 by entering the **set network failover ena** command.

```
admin: set network failover ena
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?
```

Step 9 When prompted, enter **yes** to confirm that you want to continue with enabling the bond.

```
Enter "yes" to continue or any other key to abort:

yes
executing ...
```

Step 10 To verify that the new IP address has taken effect, and that Ethernet 0 and Ethernet 1 are bonded together, enter the **show network failover** command.

```
admin: show network failover
Bond 0
DHCP         : disabled           Status     : up
IP Address   : 10.22.139.106     IP Mask    : 255.255.255.240
Link Detected: no                 Mode       : Auto disabled, N/A, N/A

Ethernet 0
DHCP         : disabled           Status     : up
IP Address   :                    IP Mask    :
Link Detected: yes                Mode       : Auto enabled, Full, 1000MB/s

Ethernet 1
DHCP         : disabled           Status     : up
IP Address   :                    IP Mask    :
Link Detected: no                 Mode       : Auto enabled, Unknown! (255), 1000MB/s

DNS
Primary      :                    Secondary  :
Options      : timeout:5 attempts:2
Domain       : localdomain
Gateway      : 10.22.139.97 on Ethernet bond0
```

What to Do Next

If you changed the IP address of an administration server, take the following actions:

- Update the real server entries on the Cisco Application Control Engine. See the "Configuring Real Servers" section on page 15-7.
- Update the firewall and any other network component that needs to be aware of the new IP address.

If you changed the IP address of a call engine server, take the following actions:

- Update the following items to reflect the new IP address:
  - Adjacencies on the Cisco Session Border Controller. See the "Creating Adjacencies" section on page 20-7.
  - Cisco Unified Communications Manager configuration on the Cisco TelePresence Multipoint Switch. See the "Configuring Unified CM Settings on the Cisco TelePresence Multipoint Switch" section on page 16-6.
  - Real server entries on the Cisco Application Control Engine. See the "Configuring Real Servers" section on page 15-7.
  - SIP trunk on the Cisco Unified Communications Manager. See the "Creating a SIP Trunk" section on page 18-4.
- Update the firewall and any other network component that needs to be aware of the new IP address.

Changing the Database VIP Address That Is Configured on a Call Engine or Administration Server

Complete this task only if you accidentally entered the wrong virtual IP (VIP) address for the database servers while you were installing a call engine or administration server.

Before You Begin

To determine whether you should complete this task, see the "Verifying Data Connectivity Among the Servers" section on page 5-18.

Procedure

Step 1 Log in to the CLI of the call engine or administration server.

Step 2 Enter the show dbip command.

```
admin: show dbip
Database IP: 10.22.128.210
```

If the IP address in the command output is not the correct VIP address of the database servers, proceed to the next step.

Step 3 Enter one of the following commands, depending on the server role:

- For a call engine server, enter the set sipserver changedbip command.
- For an administration server, enter the set adminserver changedbip command.

```
admin: set adminserver changedbip 10.22.128.234
Database server IP address has been changed to 10.22.128.234
Please restart the Admin server using the 'utils service adminserver stop|start' command
for the change to take effect
```

Step 4 Enter one of the following commands, depending on the server role:

- For a call engine server, enter the utils service sipserver stop command.
- For an administration server, enter the utils service adminserver stop command.

```
admin: utils service adminserver stop
adminserver..............Stopped
```

Step 5 Enter one of the following commands, depending on the server role:

- For a call engine server, enter the utils service sipserver start command.
- For an administration server, enter the utils service adminserver start command.

```
admin: utils service adminserver start
adminserver..............Started - PID <23338>
```

Step 6 Enter one of the following commands, depending on the server role:

- For a call engine server, enter the utils service sipserver status command.
- For an administration server, enter the utils service adminserver status command.

You may need to wait for a few minutes and repeat the command entry to see the status change to running.

```
admin: utils service adminserver status
adminserver..............Starting - PID <23338>
admin: utils service adminserver status
adminserver..............Running - PID <23338>
```

Related Topics

- Command Reference, page C-1

Configuring SIP Load Balancing on the Call Engine Servers

The Cisco Application Control Engine (ACE) is the SIP load balancer for the Cisco TelePresence Exchange System. Typically, the virtual IP (VIP) address and port of the SIP load balancer are configured only during the installation of the call engine servers. Nevertheless, you may use the following tasks to change the configuration after installation:

- Configuring the Virtual IP Address and Port for the SIP Load Balancer, page 28-5
- Displaying the Virtual IP Address and Port for the SIP Load Balancer, page 28-6
- Disabling SIP Load Balancing, page 28-6

Configuring the Virtual IP Address and Port for the SIP Load Balancer

Complete this procedure on the call engine servers to configure the SIP load balancer VIP address and port.

Before You Begin

Completing this task requires that you restart the call engine server.

Procedure

Step 1 Log in to the CLI of the call engine server.

Step 2 Enter the following command, specifying the SIP load balancer VIP. If you want to use a port other than the default 5060, then also specify the port:

set sipserver siplb ena *ip-address* [*port*]

```
admin: set sipserver siplb ena 192.0.2.25
SIP Loadbalancing is not configured on this engine.
SIP Load Balancer address has been changed to 192.0.2.25
SIP Load Balancer port has been changed to 5060
Please restart the SIP server using the 'utils service sipserver stop|start' command for
the change to take effect
```

If the system reports that SIP load balancing is already enabled, first complete the procedure in the "Configuring the Virtual IP Address and Port for the SIP Load Balancer" section on page 28-5, and then retry this step.

Step 3 Restart the call engine server by completing the following actions:

a. Stop the call engine server by entering the **utils service sipserver stop** command.

```
admin: utils service sipserver stop
sipserver.............................Stopped
```

b. Start the call engine server by entering the **utils service sipserver start** command.

```
admin: utils service sipserver start
sipserver.............................Starting - PID <32367>
```

c. Verify that the call engine server is running by entering the **utils service sipserver status** command.

```
admin: utils service sipserver status
sipserver.............................Starting - PID <32367>
admin: utils service sipserver status
sipserver.............................Running - PID <32367>
```

Step 4 Repeat this procedure on the redundant call engine server.

Verifying

Complete the procedure in the "Displaying the Virtual IP Address and Port for the SIP Load Balancer" section on page 28-6.

Displaying the Virtual IP Address and Port for the SIP Load Balancer

Complete this procedure on the call engine servers to display the configured SIP load balancer VIP address and port. If not configured, then SIP load balancing is disabled on the Cisco TelePresence Exchange System.

Procedure

Step 1 Log in to the CLI of the call engine server.

Step 2 Enter the **show siplb** command.

In the following example, SIP load balancing is enabled on the server:

```
admin: show siplb
SIP Loadbalancer Host: 192.0.2.25
SIP Loadbalancer Port: 5060
```

In the following example, SIP load balancing is disabled on the server:

```
admin: show siplb
SIP Loadbalancer is not enabled/configured on this server.
```

Disabling SIP Load Balancing

Complete this procedure on the call engine servers to disable SIP load balancing for the Cisco TelePresence Exchange System. Doing so removes the SIP load balancer VIP address and port configuration on the call engine servers.

Before You Begin

Completing this task requires that you restart the call engine server.

Procedure

Step 1 Log in to the CLI of the call engine server.

Step 2 Enter the **set sipserver siplb dis** command.

```
admin: set sipserver siplb dis
SIP Loadbalancing has been disabled.
Please restart the SIP server using the 'utils service sipserver stop|start' command for
the change to take effect
```

Step 3 Restart the call engine server by completing the following actions:

a. Stop the call engine server by entering the **utils service sipserver stop** command.

```
admin: utils service sipserver stop
sipserver.............................Stopped
```

b. Start the call engine server by entering the **utils service sipserver start** command.

```
admin: utils service sipserver start
sipserver.........................Starting - PID <32367>
```

c. Verify that the call engine server is running by entering the **utils service sipserver status** command.

```
admin: utils service sipserver status
sipserver.........................Starting - PID <32367>
admin: utils service sipserver status
sipserver........................Running - PID <32367>
```

Step 4 Repeat this procedure on the redundant call engine server.

Verifying

Complete the procedure in the "Displaying the Virtual IP Address and Port for the SIP Load Balancer" section on page 28-6.

Related Topics

- Configuring the Virtual IP Address and Port for the SIP Load Balancer, page 28-5

Changing the IMM Interface Configuration

Complete this task only if you want to change the IP address or network configuration for the integrated management module (IMM) of a Cisco TelePresence Exchange System server, for example, if you move the server into a different subnet or otherwise need to change the IP address.

Before You Begin

- This task applies only if you had previously set up the IMM interface on the server. See the "Setting Up the IMM" section on page 4-7.
- Complete this task by using one of the following web browsers:
  - Microsoft Internet Explorer version 6.0 or later with the latest Service Pack
  - Mozilla Firefox version 1.5 or later
- Make sure that the browser allows popup windows from the IMM.

Procedure

Step 1 Log in to the IMM web interface.

Step 2 Select **System > IMM Control > Network Interfaces**.

Step 3 Confirm the following field settings:

- Interface—**Enabled**
- DHCP—**Disabled - Use static IP configuration**

Step 4 Enter the new IP address, subnet mask, and default gateway IP address for the IMM interface.

Step 5 Click **Save**.

Step 6 Click **OK**.

Step 7 Select **System > IMM Control > Restart IMM**.

Step 8 Click **Restart**.

Step 9 Click **OK**.

PART 6

Troubleshooting the Cisco TelePresence Exchange System

CHAPTER 29

Password Recovery

Use this procedure to recover the administrator password, which is used to access the CLI of a Cisco TelePresence Exchange System server. This password is initially set while installing the server.

Note

- To change a known administrator password, use the set password admin command instead of performing the password recovery procedure.
- You cannot use the password recovery procedure to recover or change the security password, which the database servers use to authenticate data requests from the other nodes, and which must be defined identically on all six nodes in the server cluster. To recover the security password, you need to reinstall all six nodes and define the new security password via the installer.

Before You Begin

- You must use the same administrator username and password on all Cisco TelePresence Exchange System servers, because the administration servers also use the administrator credentials over SSH to get the status of all nodes in the server cluster.
- During this procedure, you need to insert the Cisco TelePresence Exchange System installation DVD into the disk drive to prove that you have physical access to the server.
- The password cannot be changed until at least 24 hours after it was created, unless you reinstall the Cisco TelePresence Exchange System software on the server.

Procedure

Step 1 Log in to the CLI of the server with the following username and password:

- Username: **pwrecovery**
- Password: **pwreset**

Step 2 The platform password reset window appears.

Step 3 Press any key to continue.

Step 4 If the disk drive contains a DVD, remove it now.

Step 5 Press any key to continue.

The system verifies that the disk drive is empty.

Step 6 Insert the Cisco TelePresence Exchange System installation DVD into the disk drive.

The system verifies that you have inserted the disk.

Step 7 At the prompt, enter **a** to reset the administrator password.

Step 8 Enter the new administrator password.

Make sure that you enter the same administrator password that is used on all nodes in the Cisco TelePresence Exchange System server cluster.

Step 9 Reenter the new administrator password.

The system verifies the strength of the new password and resets it.

Step 10 At the prompt, press any key to exit the password reset utility.

Step 11 Verify that the new password works by logging in to the CLI.

CHAPTER 30

Split Brain Recovery

Split brain mode refers to a state in which each database server does not know the high availability (HA) role of its redundant peer, and cannot determine which server currently has the primary HA role. In split brain mode, data modifications may have been made on either node, and those changes may not be replicated to the peer. Also, neither or both nodes may be functioning in the primary HA role.

Split brain mode occurs when there is a temporary failure of the network connections between the two database servers, for example, due to one of the following occurrences:

- Restart of either database server during synchronization.
- Physical disconnection of the Ethernet cables from a database server.
- Loss of power to one or both database servers.

Note If three or more servers failed, see the "Recovering from a Situation Where Three or More Servers Failed" section on page 33-1.

This chapter includes the following topics:

Diagnosing Split Brain Mode

Use this procedure to determine whether your database servers are in split brain mode.

Before You Begin

Make sure that the database servers are correctly cabled. See the "Cabling Requirements for the Database Servers" section on page 4-3.

Procedure

Step 1 Log in to the CLI of each database server.

Step 2 On each database server, enter the **utils service database status** command.

Step 3 If the output indicates the role values as Primary/Secondary and Secondary/Primary with only one server having the current role value as Primary, the database servers are not in split brain mode.

The following split brain conditions are listed:

- The role values display one of the following combinations:
  - The Connection Sync Status field is "StandAlone."
  - "Primary/Unknown" on one server and "Secondary/Unknown" on the other server.
  - "Secondary/Secondary" on both servers—In this particular case, if the connection sync status on both servers is "Connected," then the MySQL database is corrupted, and the split brain recovery procedure will not help. Instead, see the "Corrupted MySQL Database Recovery" chapter.
- "Secondary/Unknown" on both servers—In this particular case, if you know that one of the database servers had a reboot during the initial synchronization process, then your database system is functioning in a mode for which the split brain recovery procedure will not help. To recover, you need to reinstall both database servers. See the "Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers" section on page 5-4.

Step 4 To recover from split brain mode, proceed to the "Recovering from Split Brain Mode" section on page 30-3.

Example

In the following example, one of the database servers is StandAlone, which indicates that the nodes are in split brain mode:

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : secondary
The current HA role of this node                 : primary
The database vip address                         : 10.22.130.54
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.49
Corosync status                                  : Running PID <18613>
Current Designated Controller (DC)               : ctx-db-2 - partition with quorum
MySQL status                                     : Running pid  2810
Connection Sync Status                           : StandAlone
Role (this-node/peer-node)                       : Primary/Unknown
Disk Status (this-node/peer-node)                : UpToDate/DUnknown
--------------------------------------------------------------------------------
```

Related Topics

- Command Reference, page C-1

Recovering from Split Brain Mode

Use this procedure to recover your database servers from split brain mode.

Before You Begin

- Complete the "Diagnosing Split Brain Mode" section on page 30-1 to confirm that your system is in split brain mode.
- Decide which node has the data that you want to keep. In this procedure, you will give this node the primary HA role. All data on the other node will be lost during this procedure and will not be recoverable.

  If you do not know which node has the most recent or most valuable data, follow these recommendations:

  – If the **utils service database status** command output on both nodes indicates that one node currently has the primary HA role while the other node currently has the secondary HA role, you should choose the current primary node to keep as the primary database server.

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : primary
The current HA role of this node                 : primary
The database vip address                         : 10.22.130.54
…
```

  – If the **utils service database status** command output on both nodes indicates that neither or both nodes have the primary HA role, choose the node that you initially installed as the primary server to keep as the primary database server.

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : primary
The current HA role of this node                 : secondary
The database vip address                         : 10.22.130.54
…
```

Procedure

Step 1 Log in to the CLI of the database server which has the data that you want to keep.

Step 2 Enter the **utils service database drbd keep-node** command to reset the server to currently function in the primary HA role.

```
admin: utils service database drbd keep-node
This command will make this node as Primary
Trying to assume primary role..... [Done]
Reconnecting to MySQL..... [Done]
```

Step 3 Log in to the CLI of the other database server.

Step 4 Enter the **utils service database drbd discard-node** command to reset the server to currently function in the secondary HA role.

```
admin: utils service database drbd discard-node
This command will make this node as Secondary
Trying to assume secondary role..... [Done]
Ensuring DRBD volume unmounted...
Ensuring DRBD role is Secondary...
Discarding local MySQL data..... [Done]
```

Synchronization begins between the two database servers.

Step 5 Proceed to the "Verifying Synchronization of the Database Servers" section on page 30-4.

Related Topics

- Command Reference, page C-1

Verifying Synchronization of the Database Servers

Procedure

Step 1 Log in to the CLI of each database server.

Step 2 On each database server, enter the **utils service database status** command.

The following examples show that synchronization is in progress and proceeding successfully, because each node is aware of the HA role of its redundant peer, and the output displays the percentage of the synchronization progress. Also, the current primary database server identifies itself as the SyncSource, while the current secondary database server identifies itself as the SyncTarget.

Sample output from the current primary database server:

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : primary
The current HA role of this node                 : primary
The database vip address                         : 10.22.130.54
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.49
Corosync status                                  : Running PID <20414>
Current Designated Controller (DC)               : ctx-db-2 - partition with quorum
MySQL status                                     : Running pid 10100
Connection Sync Status                           : SyncSource
Role (this-node/peer-node)                       : Primary/Secondary
Disk Status (this-node/peer-node)                : UpToDate/Inconsistent
```

Sample output from the current secondary database server:

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : secondary
The current HA role of this node                 : secondary
The database vip address                         : 10.22.130.54
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.49
Corosync status                                  : Running PID <17842>
Current Designated Controller (DC)               : ctx-db-2 - partition with quorum
MySQL status                                     : Not running (only runs on database
server with current role primary.)
Connection Sync Status                           : SyncTarget
Role (this-node/peer-node)                       : Secondary/Primary
Disk Status (this-node/peer-node)                : Inconsistent/UpToDate
--------------------------------------------------------------------------------
```

Note The synchronization takes approximately 40 minutes. During this time, the disk status value of the current secondary server is shown as **inconsistent**. An inconsistent disk state indicates that the synchronization between the database servers is not complete.

Step 3 To confirm that the synchronization is complete, enter the **utils service database status** command on both the primary and secondary database servers.

The following examples show that synchronization is complete, because the disk status of the current secondary server is now up to date.

Sample output from the primary database server:

```
admin: utils service database status
------------------------------------------------------------------------------
The initial configured HA role of this node      : primary
The current HA role of this node                 : primary
The database vip address                         : 10.22.130.54
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.49
Corosync status                                  : Running PID <20414>
Current Designated Controller (DC)               : ctx-db-2 - partition with quorum
MySQL status                                     : Running pid 10100
Connection Sync Status                           : Connected
Role (this-node/peer-node)                       : Primary/Secondary
Disk Status (this-node/peer-node)                : UpToDate/UpToDate
------------------------------------------------------------------------------
```

Sample output from the secondary database server:

```
admin: utils service database status
------------------------------------------------------------------------------
The initial configured HA role of this node      : secondary
The current HA role of this node                 : secondary
The database vip address                         : 10.22.130.54
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.49
Corosync status                                  : Running PID <17842>
Current Designated Controller (DC)               : ctx-db-2 - partition with quorum
MySQL status                                     : Not running (only runs on database
server with current role primary.)
Connection Sync Status                           : Connected
Role (this-node/peer-node)                       : Secondary/Primary
Disk Status (this-node/peer-node)                : UpToDate/UpToDate
------------------------------------------------------------------------------
```

Tip If this verification procedure shows that the split brain recovery procedure did not work for either or both servers, proceed to the "Diagnosing Corrupted DRBD Metadata" section on page 30-6.

Diagnosing Corrupted DRBD Metadata

If, after you complete the split brain recovery procedure, the database servers still cannot connect to each other and complete synchronization, the metadata for the Distributed Replicated Block Device (DRBD) may be corrupted. The DRBD is what synchronizes the secondary database with changes that are made on the primary database.

Before You Begin

This procedure applies only after you attempt split brain recovery. (See the "Recovering from Split Brain Mode" section on page 30-3.)

Procedure

Step 1 Log in to the CLI of each database server.

Step 2 On each database server, enter the **utils service database status** command.

Step 3 The DRBD metadata is corrupted if the disk status value is "Inconsistent/Inconsistent" while the connection sync status is "StandAlone" or "WFConnection" on one or both servers.

Step 4 To recover from corrupted DRBD metadata, proceed to the "Recovering from Corrupted DRBD Metadata" section on page 30-6.

Example

In the following example, the status of one database server indicates that the nodes have corrupted DRBD metadata:

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : secondary
The current HA role of this node                 : secondary
The database vip address                         : 10.22.130.54
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.49
Corosync status                                  : Running PID <11459>
Current Designated Controller (DC)               : ctx-db-2 - partition with quorum
MySQL status                                     : Not running (only runs on database
server with current role primary.)
Connection Sync Status                           : WFConnection
Role (this-node/peer-node)                       : Secondary/Unknown
Disk Status (this-node/peer-node)                : Inconsistent/Inconsistent
--------------------------------------------------------------------------------
```

Related Topics

- Command Reference, page C-1

Recovering from Corrupted DRBD Metadata

Before You Begin

- Make sure that the database servers are correctly cabled. See the "Cabling Requirements for the Database Servers" section on page 4-3.

- Complete the "Diagnosing Corrupted DRBD Metadata" section on page 30-6 to confirm that your system has corrupted DRBD metadata.

Procedure

Step 1 Log in to the CLI of the database server which has the data that you want to keep.

This should be the same node whose data you decided to keep when you completed the procedure in the "Recovering from Split Brain Mode" section on page 30-3.

Step 2 Enter the **utils service database drbd force-keep-node** command to reset the DRBD metadata and set the server to currently function in the primary HA role.

```
admin: utils service database drbd force-keep-node
This command will make this node as Primary
Trying to assume primary role......... [Done]
Overwriting peer data... [Done]
```

Step 3 Log in to the CLI of the other database server.

Step 4 Enter the **utils service database drbd force-discard-node** command to reset the DRBD metadata and set the server to currently function in the secondary HA role.

```
admin: utils service database drbd force-discard-node
Shutting down Heartbeat...
Stopping High-Availability services:
[  OK  ]
Ensuring DRBD volume unmounted...
umount: /dev/drbd0: not mounted
Taking down DRBD Resource...
Recreating DRBD meta-data...
NOT initialized bitmap
Bringing up DRBD...
Starting Heartbeat...
Starting High-Availability services:
[  OK  ]
 [Done]
```

Synchronization begins between the two database servers.

Step 5 Proceed to the "Verifying Synchronization of the Database Servers" section on page 30-4.

Related Topics

- Command Reference, page C-1

CHAPTER 31

Corrupted MySQL Database Recovery

This chapter includes the following sections:

Diagnosing a Corrupted MySQL Database

Use this procedure to determine whether your database servers have a corrupted MySQL database.

Procedure

Step 1 Log in to the CLI of each database server.

Step 2 On each database server, enter the **utils service database status** command.

Step 3 If the output indicates the following conditions, then the database servers have a corrupted MySQL database.

- The Connection Sync Status field is "Connected."
- The disk status value is "Inconsistent/Inconsistent."
- The role values are "Secondary/Secondary" on both servers.
- The current HA role is "secondary" for both servers.

Because both servers have the secondary HA role, the MySQL database cannot run.

Step 4 To recover from a corrupted MySQL database, proceed to the "Recovering from a Corrupted MySQL Database" section on page 31-2.

Example

In the following example, the status indicates that the nodes have a corrupted MySQL database.

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : secondary
The current HA role of this node                 : secondary
The database vip address                         : 10.22.130.54
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.49
Corosync status                                  : Running PID <19984>
```

```
Current Designated Controller (DC)              : ctx-db-2 - partition with quorum
MySQL status                                    : Not running (only runs on database
server with current role primary.)
Connection Sync Status                          : Connected
Role (this-node/peer-node)                      : Secondary/Secondary
Disk Status (this-node/peer-node)               : UpToDate/UpToDate
--------------------------------------------------------------------------------
```

Related Topics

- Command Reference, page C-1

Recovering from a Corrupted MySQL Database

Before You Begin

- Make sure that the database servers are correctly cabled. See the "Cabling Requirements for the Database Servers" section on page 4-3.
- Complete the "Diagnosing a Corrupted MySQL Database" section on page 31-1 to confirm that your system has a corrupted MySQL database.
- From the administration console, back up the database. See the "Performing a Manual Database Backup" section on page 24-3.

Caution All data in the MySQL database will be lost during this procedure and will not be recoverable.

Procedure

Step 1 Log in to the CLI of the database server that you want to have the primary HA role.

Step 2 Enter the **utils service database drbd force-mysql-reset** command.

```
admin: utils service database drbd force-mysql-reset
This command will make this node as Primary
This command will make this node as Primary
Trying to assume primary role..... [Done]
Temporarily stopping mon services...
Stopping mon daemon: [FAILED]
Stopping MySQL...
 ERROR! MySQL manager or server PID file could not be found!
Ensuring DRBD volume unmounted...
Rebuilding DRBD filesystem...
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
5898240 inodes, 11796480 blocks
589824 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=12582912
360 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424
```

```
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 21 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
Remounting DRBD volume...
Retrieving backup MySQL files...
Starting MySQL...
Starting MySQL. ERROR! Manager of pid-file quit without updating file.
Starting mon...
Starting mon daemon: [  OK  ]
 [Done]
```

The server then restarts, is assigned the primary HA role, and initiates the synchronization process.

What To Do Next

From the administration console, restore the database. See the "Restoring a Database Server Backup" section on page 24-4.

CHAPTER 32

Troubleshooting Calls and Meetings

This chapter describes issues with troubleshooting calls, and includes the following topics:

Troubleshooting Interop Calls

Interop endpoints are single and three-screen endpoints that are H.323 and ISDN standards-based. All interop calls are routed through the hosted Cisco VCS.

When there are problems with guest dialout calls or when an interop call drops, there are a number of steps that you can take to isolate the cause of the problem.

Procedure

To troubleshoot an interop call, do the following procedure:

Step 1 Log in to the Cisco TelePresence Exchange System.

Step 2 From the navigation pane, choose **Collaboration Services > Meetings**.

The Meetings window is displayed.

Step 3 Click the applicable meeting to go to the Meeting Details page.

Step 4 From the toolbar, click **Go to Diagnostics**.

The Meeting Diagnostics page is displayed.

Step 5 In the search results, determine when each dialout participant joined and left the call, and the disconnect reason for the call.

Look for endpoints that were disconnected before the end of the meeting time, or for abnormal disconnect reasons such as rejected or resource shutdown. These issues generally indicate that an endpoint is unable to join a meeting.

Step 6 Log in to the Cisco VCS as the administrator.

Step 7 From the tool bar, choose **Status > Calls > History**.

The Call History window is displayed.

Step 8 In the Status column, look at the status of the interop call that is experiencing problems.

- When the call status shows that the call was rejected, determine if the call was routed to the right destination. If not, identify and fix the routing issue on the Cisco VCS.

  For additional information on the Cisco VCS, see http://www.cisco.com/en/US/products/ps11337/tsd_products_support_series_home.html.

- When the call status indicates normal call clearing, the problem is not with the Cisco VCS.

  To further diagnose the problem, select one of the following options:

  - For guest dialout calls to ISDN endpoints, check the status of the call on the Cisco TelePresence ISDN Gateway MSE 8321 resource.

    For additional information on the Cisco TelePresence ISDN Gateway MSE 8321, see http://www.cisco.com/en/US/products/ps11340/tsd_products_support_series_home.html.

  - For ISDN calls, verify that the prefix of the endpoint does not match the ISDN Dialout Prefix configured on the System > Global Configuration window. Also verify that the ISDN Dialout Prefix is not set to null and that it matches the value that is configured within the Cisco VCS.

    See the "Configuring an ISDN Dial Out Prefix" section on page 8-11 for information on changing the ISDN Dialout Prefix.

  - For dialout calls placed on enterprise endpoints, check the status of the call on the session border controller (SBC).

  - For URI and IP dialout calls, check the status of the call on the Cisco TelePresence Video Communication Server Expressway.

    For additional information on the Cisco VCS Expressway, see http://www.cisco.com/en/US/products/ps11337/tsd_products_support_series_home.html.

- When there is no record of the call on the Cisco VCS, check the status of the call on the appropriate Cisco TelePresence MSE 8000 Series resource in the network (Cisco TelePresence Server MSE 8710 or Cisco TelePresence MCU MSE 8510), and use a static meeting to test why a dialout to an endpoint is failing.

  For additional information on the Cisco MSE 8000 Series, see http://www.cisco.com/en/US/products/ps11340/tsd_products_support_series_home.html.

Troubleshooting Failure of an Endpoint to Call into a Second Meeting

The system allows an endpoint to participate in only one meeting at a time. Therefore, when an endpoint is currently in a meeting, it is not permitted to simultaneously join a second meeting.

Below are examples of instances when a user may not be able to call in to a second meeting:

- The user places the call on hold while in a meeting, and attempts to call into a second meeting. Because the system does not support simultaneous connection to more than one meeting, the user must remove the call from hold before attempting to join another meeting.

- From the system perspective, the endpoint has disconnected abnormally from a meeting and appears to still be connected. From the user perspective, the endpoint currently has no calls that are active or on hold. To help resolve this problem, where the call appears to still be in session from a previous meeting because the endpoint was disconnected abnormally, complete the following procedure:

Procedure

Step 1 From the endpoint that was in the first meeting, try to rejoin that meeting.

Step 2 After successfully rejoining the meeting, end the call as you normally would.

Step 3 Try to join the second meeting.

If this procedure does not resolve the issue and you are still unable to join another meeting, wait until the scheduled end of the first meeting and try again.

Troubleshooting Failure of an EX or C-Series Endpoint to Call into a Meeting Hosted on a CTMS Media Resource

If calls from a Cisco TelePresence endpoint running TC release 5.x (for example, C20/C60/C90, EX60, or Ex90) fail when the endpoint attempts to connect to a meeting hosted on a Cisco TelePresence Multipoint Switch (CTMS), check the value of the Default Call Rate parameter on the endpoint. The CTMS rejects calls that use the default value of the parameter in TC release 5.x (768 kbps) as having insufficient bandwidth. The minimum call rate when dialing in to a CTMS is 2250 kbps. We recommend setting a value of at least 4000 kbps.

Refer to the endpoint documentation for instructions on changing the Default Call Rate parameter. For more information on the issue, see https://supportforums.cisco.com/docs/DOC-23082.

Troubleshooting Smallest Capacity Exceeded Failure when Scheduling a Meeting

If the Cisco TelePresence Exchange System returns the error message “Meeting capacity has exceeded the smallest capacity size available for resource type <Bridge Type>” when you attempt to schedule a meeting, and you have multiple media resources of the listed bridge type, you may need to check the configuration of each media resource of that type, and “level” the Max Capacity setting on each.

When the system attempts to reserve capacity for the meeting at scheduling time, it checks both the size of the pool of resources and the Max Capacity setting of each media resource. Because the system does not actually allocate resources on a specific bridge until the meeting begins, it must ensure that even the smallest bridge resource in the pool can handle the meeting size, in case an insufficient amount of capacity is available on the larger bridges.

If, for example, you have three CTMS resources, two of which have Max Capacity set to 48 and a third which has Max Capacity set to 4, and the meeting requires 6 segments, the system will not be able to schedule the meeting on that bridge type because the smallest bridge cannot handle the meeting capacity. In this case, you will need to either even out the Max Capacity values across the resources, or delete the smallest resource, in order to schedule the meeting. In other words, to handle the 6-segment meeting reservation, there must not be any resources configured with Max Capacity set to less than 6.

For information on configuring Max Capacity for a media resource, see Chapter 9, “Configuring Media Resources.”

CHAPTER 33

Server Failure Recovery

This chapter includes the following sections:

Recovering from a Situation Where Three or More Servers Failed

To recover from this situation, see the following tasks:

Disabling High Availability to Enable the Current Secondary Database Server to Take Over the Primary Role

For a database server to retain the primary high availability (HA) role, a minimum of four Cisco TelePresence Exchange System nodes must be online. If three nodes are offline (for example, one administration server, one call engine server, and one failed database server), the remaining database server cannot act as the primary database server. Therefore, you must use the **utils service database drbd disable-ha** command to allow a database server to assume the primary role. This situation allows a database server to assume the primary HA role even when it did not meet the minimum quorum of four votes. After you have four or more Cisco TelePresence Exchange System nodes available, use the **utils service database drbd enable-ha** command to bring the system back to the original configuration.

Procedure

Step 1 Log in to the CLI of the database server that is still working.

Step 2 Enter the **utils service database status** command to verify that the node has not already taken over the primary HA role.

```
admin: utils service database status
--------------------------------------------------------------------------------
```

```
The initial configured HA role of this node      : primary
The current HA role of this node                 : secondary
The database vip address                         : 10.22.130.54
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.49
Corosync status                                  : Running PID <17337>
Current Designated Controller (DC)               : ctx-db-2 - partition with quorum
MySQL status                                     : Not running (only runs on database
server with current role primary.)
Connection Sync Status                           : WFConnection
Role (this-node/peer-node)                       : Secondary/Unknown
Disk Status (this-node/peer-node)                : UpToDate/Unknown
--------------------------------------------------------------------------------
```

Note If the current HA role is primary, do not complete the rest of this procedure. You already have a working current primary database server. If the failed server needs to be replaced, proceed to the "Replacing a Database Server" section on page 33-3.

Step 3 Enter **utils service database drbd disable-ha**.

```
admin: utils service database drbd disable-ha
Disabling quorum requirement... [Done]
```

Step 4 Enter the **utils service database status** command to verify that the node takes over the primary HA role.

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : primary
The current HA role of this node                 : primary
The database vip address                         : 10.22.130.54
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.49
Corosync status                                  : Running PID <18030>
Current Designated Controller (DC)               : ctx-db-2 - partition with quorum
MySQL status                                     : Running pid 20445
Connection Sync Status                           : WFConnection
Role (this-node/peer-node)                       : Primary/Unknown
Disk Status (this-node/peer-node)                : UpToDate/Unknown
--------------------------------------------------------------------------------
```

You may need to wait a few minutes for the current HA role to change to "primary" and for the MySQL database to become available (MySQL status of "Running").

Step 5 If the **MySQL status** continues to show the value "Not running," enter the **utils service database drbd keep-node** command:

```
admin: utils service database drbd keep-node
This command will make this node as Primary
Trying to assume primary role..... [Done]
Reconnecting to MySQL..... [Done]
```

What To Do Next

Determine whether or not the other database server can be recovered.

- If the server can be recovered, proceed to the "Enabling HA After Recovering a Database Server" section on page 33-3.
- If the server cannot be recovered, proceed to the "Replacing a Database Server" section on page 33-3.

Related Topics

- Command Reference, page C-1

Enabling HA After Recovering a Database Server

Before You Begin

- Complete this task only if you had previously completed the procedure in the "Disabling High Availability to Enable the Current Secondary Database Server to Take Over the Primary Role" section on page 33-1.
- Do not complete this task for a replacement server. Instead, see the "Replacing a Database Server" section on page 33-3.

Caution This procedure will temporarily interrupt MySQL service. Cisco recommends that you complete this task during a maintenance window. During the MySQL service interruption, new calls will not be able to connect to meetings, and users will not be able to schedule meetings.

Procedure

Step 1 Turn off the recovered server.

Step 2 Log in to the CLI of the current primary database server.

Step 3 Enter **utils service database drbd enable-ha**.

```
admin: utils service database drbd enable-ha
Enabling quorum requirement... [Done]
```

Step 4 After the reboot is complete, verify that the database servers are not in split brain mode. See the "Diagnosing Split Brain Mode" section on page 30-1.

Related Topics

- Command Reference, page C-1

Replacing a Database Server

See the following sections:

- Preparing to Replace a Database Server, page 33-4
- Setting Up the Replacement Database Server, page 33-5
- Installing the Software on the Replacement for the Initial Secondary Database Server, page 33-5
- Installing the Software on the Replacement for the Initial Primary Database Server, page 33-6

Preparing to Replace a Database Server

Procedure

Step 1 Obtain the Cisco TelePresence Exchange System installation DVD, or download the software from the following URL and burn the disk image onto a DVD: http://www.cisco.com/go/ctx-download.

Note Verify that the software version on the installation DVD is the same as the version that is currently running on the peer server of the same role. If you want to upgrade the software, you may do so after you successfully replace the failed server.

Step 2 Find your completed Appendix A, "Installation Worksheets," from when you installed the Cisco TelePresence Exchange System.

If you cannot find your completed worksheet, or if the information has become obsolete, gather the following information for the database server:

- Hostname, IP address, and subnet mask of the individual database server.
- Hostname, virtual IP (VIP) address, and subnet mask that are shared by both database servers.
- Default gateway.
- Administrator username and password—These are used to access the CLI on the server. You must use the same administrator username and password on all Cisco TelePresence Exchange System servers, because the administration servers also use the administrator credentials over SSH to get the status of all nodes in the server cluster.
- Security password—You must use the same security password that is defined on all of the other Cisco TelePresence Exchange System servers. The database server uses this password to authenticate data requests from the administration and call engine servers.
- Information for generating the locally significant certificate (LSC):
  - Organization—typically your company name.
  - Unit—typically your business unit and department.
  - Location—typically the building, floor, and rack in which the server is installed.
  - State and Country—where the server is located.

  Use the following guidelines to determine each entry for generating LSCs:
  - Refer to your company guidelines for format and entry requirements.
  - Supported characters include alphanumeric, space, and the following special characters: .,-_:;{}()[]#.
  - Each field supports up to 255 characters.
- IP addresses, hostnames, or pool names for external Network Time Protocol (NTP) clocking sources—You must configure the same NTP entries that are defined on all of the other Cisco TelePresence Exchange System servers.

Optionally, gather the following information for the integrated management module (IMM) interface, which enables remote control of the server:

- IP address and subnet mask
- Default gateway
- Username and password

Setting Up the Replacement Database Server

Before You Begin

Complete the procedure in the "Replacing a Database Server" section on page 33-3.

Procedure

Step 1 Follow the hardware installation instructions for the server to properly rack mount the server.

Also see the "Recommendations for Rack Mounting the Cisco TelePresence Exchange System and Other Solution Components" section on page 4-2.

Step 2 Connect the power, network, and console access cables to the server. See Cabling Requirements for the Database Servers, page 4-3.

Step 3 (Optional) Set up the IMM interface for remote control of the server.

See the "Setting Up the IMM" section on page 4-7.

Step 4 Proceed to one of the following sections, depending on the initial HA role of the database server that you are replacing:

- Installing the Software on the Replacement for the Initial Secondary Database Server, page 33-5
- Installing the Software on the Replacement for the Initial Primary Database Server, page 33-6

Step 5 Proceed to the "Verifying Data Connectivity Among the Servers" section on page 5-18.

Installing the Software on the Replacement for the Initial Secondary Database Server

Before You Begin

Complete the procedure in the "Setting Up the Replacement Database Server" section on page 33-5.

Caution This procedure will temporarily interrupt MySQL service. Cisco recommends that you complete this task during a maintenance window. During the MySQL service interruption, new calls will not be able to connect to meetings, and users will not be able to schedule meetings.

Procedure

Step 1 Install the software on the replacement server. See the "Installing the Database Server Software" section on page 5-4.

Note Make sure that you enter **No** when the installer asks whether to configure this node as the primary database server.

Step 2 Verify that the initial configured HA role of this node is **secondary**.

See the "Checking the Initial High-Availability Roles of the Database Servers" section on page 5-7.

Step 3 Log in to the CLI of the current primary database server.

Step 4 Enter **utils service database drbd enable-ha**.

```
admin: utils service database drbd enable-ha
Enabling quorum requirement... [Done]
```

Note This step is required only if you disabled HA by using the **utils service database drbd disable-ha** command.

Step 5 Enter the **utils service database status** command.

If the database servers are not synchronized, see the "Split Brain Recovery" chapter.

Related Topics

- Command Reference, page C-1

Installing the Software on the Replacement for the Initial Primary Database Server

Before You Begin

Complete the procedure in the "Replacing a Database Server" section on page 33-3.

Caution This procedure will temporarily interrupt MySQL service. Cisco recommends that you complete this task during a maintenance window. During the MySQL service interruption, new calls will not be able to connect to meetings, and users will not be able to schedule meetings.

Procedure

Step 1 Install the software on the replacement server. See the "Installing the Database Server Software" section on page 5-4.

Note Make sure that you enter **Yes** when the installer asks whether to configure this node as the primary database server.

Step 2 Verify that the initial configured HA role of this node is primary by entering **utils service database status**.

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : primary
The current HA role of this node                 : secondary
The database vip address                         : 10.22.163.218
Node name                                        : intersp-db1
Node IP address                                  : 10.22.163.216
Corosync status                                  : Running PID <23905>
Current Designated Controller (DC)               : intersp-eng2 - partition with quorum
MySQL status                                     : Not running (only runs on database
server with current role primary.)
Connection Sync Status                           : SyncTarget 2.7%
Role (this-node/peer-node)                       : Secondary/Primary
Disk Status (this-node/peer-node)                : Inconsistent/UpToDate
--------------------------------------------------------------------------------
```

After the synchronization process is complete, the disk status value will be changed to UpToDate/UpToDate.

Step 3 Log in to the CLI of the current primary database server.

Step 4 Enter **utils service database drbd enable-ha**.

Note This step is required only if you disabled HA by using the **utils service database drbd disable-ha** command.

```
admin: utils service database drbd enable-ha
Enabling quorum requirement... [Done]
```

What to Do Next

Complete the following procedures:

- Checking the Network Connectivity of the Database Servers, page 5-9
- Verifying Data Connectivity Among the Servers, page 5-18

Related Topics

- Command Reference, page C-1

Replacing an Administration or Call Engine Server

Procedure

Step 1 Obtain the Cisco TelePresence Exchange System installation DVD, or download the software from the following URL and burn the disk image onto a DVD: http://www.cisco.com/go/ctx-download.

Note Verify that the software version on the installation DVD is the same as the version that is currently running on the peer server of the same role. If you want to upgrade the software, you may do so after you successfully replace the failed server.

Step 2 Find your completed Appendix A, "Installation Worksheets," from when you installed the Cisco TelePresence Exchange System.

If you cannot find your completed worksheet, or if the information has become obsolete, gather the following information for the server that you need to replace:

- Hostname
- IP address and subnet mask
- Default gateway
- Administrator username and password—These are used to access the CLI on the server. You must use the same administrator username and password on all Cisco TelePresence Exchange System servers, because the administration servers also use the administrator credentials over SSH to get the status of all nodes in the server cluster.
- Security password—You must use the same security password that is defined on all of the other Cisco TelePresence Exchange System servers. The database server uses this password to authenticate data requests from the administration and call engine servers.
- Information for generating the locally significant certificate (LSC):
  - Organization—typically your company name.
  - Unit—typically your business unit and department.
  - Location—typically the building, floor, and rack in which the server is installed.
  - State and Country—where the server is located.

  Use the following guidelines to determine each entry for generating LSCs:
  - Refer to your company guidelines for format and entry requirements.
  - Supported characters include alphanumeric, space, and the following special characters: .,-_:;{}()[]#.
  - Each field supports up to 255 characters.

Optionally, gather the following information for the integrated management module (IMM) interface, which enables remote control of the server:

- IP address and subnet mask
- Default gateway
- Username and password

Step 3 Follow the hardware installation instructions for the server to properly rack mount the server.

Also see the "Recommendations for Rack Mounting the Cisco TelePresence Exchange System and Other Solution Components" section on page 4-2.

Step 4 Connect the power, network, and console access cables to the server.

See the "Cabling Requirements for the Administration and Call Engine Servers" section on page 4-4.

Step 5 (Optional) Set up the IMM interface for remote control of the server.

See the "Setting Up the IMM" section on page 4-7.

Step 6 Install the software by using one of the following sections:

- Installing the Cisco TelePresence Exchange System Call Engine Servers, page 5-9
- Installing the Cisco TelePresence Exchange System Administration Servers, page 5-14

Step 7 Proceed to the "Verifying Data Connectivity Among the Servers" section on page 5-18.

CHAPTER 34

Logs

You can access the Cisco TelePresence Exchange System logs via these CLI commands:

- **file dump**—Displays the contents of one or more files on the screen, one page at a time.
- **file get**—Retrieves files using SSH file transfer protocol (SFTP).
- **file list**—Lists the files and subdirectories that are in a specified directory.
- **file search**—Searches the content of log files and displays the lines that match a specified regular expression.
- **file tail**—Displays the most recent entries in a log file and any additional logs as they are written into the file.
- **file view**—Displays the contents of a file.

Obtaining Logs for a Customer Service Representative

If a customer service representative requests the logs for your system, complete this procedure to use SSH File Transfer Protocol (SFTP) to transfer to logs from each server to an external machine (SFTP server). You can then send the log files to the customer service representative.

Before You Begin

Obtain the following information about the SFTP server:

- IP address
- Port
- User ID
- Password
- Target directory

Procedure

Step 1 Log in to the CLI of the server.

Step 2 Enter **file get activelog ctc/log/*.log** and follow the prompts.

```
admin: file get activelog ctc/log/*.log
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 5
```

```
Total size in Bytes: 180218286
Total size in Kbytes: 175994.42
Would you like to proceed [y/n]? y
SFTP server IP: 10.22.140.75
SFTP server port [22]:
User ID: root
Password: ********

Download directory: /tmp

.....
Transfer completed.
:
```

Step 3 Repeat this procedure for each node in the Cisco TelePresence Exchange System server cluster whose logs are requested by the customer support representative.

Step 4 Send the log files to the customer support representative.

PART 7

Appendixes

APPENDIX A

Installation Worksheets

Complete these worksheets before you install the software on the Cisco TelePresence Exchange System database, administration, and call engine servers. For details and requirements, see the "Gathering Required Information Before Installation" section on page 4-5.

Table A-1 Worksheet for Cisco TelePresence Exchange System Servers

Node	Hostname	IP Address	Subnet Mask	Username	Password
Database—shared virtual[1]				—	—
Database—primary				—	—
Database—secondary				—	—
Engine 1				—	—
Engine 2				—	—
Admin 1				—	—
Admin 2				—	—
Default gateway for the data VLAN			—	—	—
Administrator username and password for accessing the CLI of any node in the cluster[2]					
Security password to authenticate data requests between the database server and the other servers[3]					
Database—primary IMM[4] (optional)	—				
Database—secondary IMM (optional)	—				
Engine 1—IMM (optional)	—				
Engine 2—IMM (optional)	—				
Admin 1—IMM (optional)	—				
Admin 2—IMM (optional)	—				
Default gateway for the IMM VLAN			—	—	—

1. The virtual hostname and virtual IP (VIP) address are shared by both the primary and secondary database servers.
2. You must use the same administrator username and password on all Cisco TelePresence Exchange System servers.
3. The security password must be identical for all nodes in the server cluster. After you set the security password on a server, you cannot change it without reinstalling the server.
4. IMM = integrated management module. Use and setup of the IMM is optional, but the IMM enables remote control of the server.

Table A-2 Worksheet for Other Solution Components

Component	Information	Value
SIP load balancer (ACE[1])	VIP[2] address	
	Port[3]	
DNS[4] (optional)	IP address of primary DNS server	
	IP address of secondary DNS server (optional)	
	Domain name[5]	
NTP[6]	Server IP address, server hostname, or pool name	
	Server IP address, server hostname, or pool name	
	Server IP address, server hostname, or pool name	
	Server IP address, server hostname, or pool name	
	Server IP address, server hostname, or pool name	

1. ACE = Cisco Application Control Engine.
2. VIP = virtual IP address.
3. Cisco recommends that you use the default port 5060.
4. DNS = Domain Name System.
5. Example domain names: cisco.com, example.net.
6. NTP = network time protocol. Only one NTP entry is required, but Cisco recommends that you have at least three clocking sources.

Table A-3 Worksheet for Generating LSCs[1] for the Cisco TelePresence Exchange System Servers

Node	Organization	Unit	Location	State	Country
Database—primary					
Database—secondary					
Engine 1					
Engine 2					
Admin 1					
Admin 2					

1. LSC = locally significant certificate

APPENDIX B

Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection

This appendix describes some key Cisco TelePresence Exchange System concepts in further depth. See the following sections:

Comparing Organization Ports and Segments of Capacity

The Cisco TelePresence Exchange System product has two differing concepts which are often confused with each other. The official terminology which is used here and in the documentation set is “ports of organization bandwidth” and “segments of capacity.” The following sections describe the two concepts in further detail:

Ports and Bandwidth

The term “port” is generally used in Cisco TelePresence Exchange System terminology to indicate a measure of the amount of network bandwidth consumed by an active endpoint, in telepresence traffic between the endpoint organization and the Cisco TelePresence Exchange System.

When you create an organization in the Cisco TelePresence Exchange System, you specify a value for the Max Ports setting, which determines the sum total amount of bandwidth that the organization's endpoints can consume at a given time.

When you schedule a Meet-Me meeting, you typically add one or more provisioned endpoints to the meeting, and you may add unprovisioned endpoints as well. When adding a provisioned or unprovisioned endpoint to the meeting, you specify the organization to which the endpoint belongs, and you can also specify the number of ports of organization bandwidth used by the endpoint. The system counts these ports toward the Max Ports value defined for the organization for the meeting time slot. If

adding the endpoint to the scheduled meeting would cause the associated organization to exceed its Max Ports value for the given time slot, the meeting scheduling will fail with an error message indicating that the organization bandwidth is exceeded.

Remote meetings function similarly to Meet-Me meetings—you can choose to reserve bandwidth towards the organization to which the endpoint belongs when scheduling the meeting.

The system only checks the organization bandwidth when you are scheduling or modifying a meeting before it has started—it does not enforce organization bandwidth at attend time. For this reason, Rendezvous meetings, which cannot have endpoint participants added at scheduling time, do not affect the bandwidth calculation for an organization.

The system does not allow you to reserve ports of organization bandwidth for the endpoints in a two-party direct meeting because this type of meeting is direct dialed between the endpoints. You schedule a two-party direct meeting in the system only in order to provide One-Button-to-Push support for the endpoints.

Placing limits on organization bandwidth at scheduling time is optional, and you can define a "port" of bandwidth according to actual endpoint traffic consumption in your network. You may choose to use the number of screens of each endpoint as your unit of measurement for the amount of bandwidth that the endpoint utilizes, or some other measure. Or you may choose to bypass the organization bandwidth management entirely by always specifying 0 (in the administration console) or null (in API calls) for the endpoint bandwidth, effectively disabling the feature.

Segments and Capacity

Capacity is a concept which refers to the amount of resources reserved or consumed on the multipoint media bridge that is hosting the meeting. The Cisco TelePresence Exchange System documentation set generally uses the term segment as a measure of the amount of capacity allocated to or used by an endpoint on a media bridge during a meeting time frame, although occasionally the term ports or ports/segments is used.

See the following sections for details on how the system reserves, allocates, and de-allocates capacity:

- Capacity Reservation Calculation for Meet-Me Meetings, page B-2
- Capacity Reservation Calculation for Rendezvous Meetings, page B-4
- Capacity Reservation and Allocation for Meet-Me and Rendezvous Meetings, page B-4
- Capacity Usage at Attend Time, page B-5
- Capacity De-allocation, page B-5

Capacity Reservation Calculation for Meet-Me Meetings

When you add a provisioned endpoint to a Meet-Me meeting, in many cases, the Cisco TelePresence Exchange System assumes that the quantity of segments required for the endpoint is equal to the number of screens specified in the media profile associated with the endpoint. There are exceptions, however, depending on the type of bridge that will host the meeting and the scenario (dial in or dial out, whether the endpoint supports 30 FPS presentation sharing, and whether or not the organization of the endpoint has the Minimize Capacity check box checked).

Table B-1 describes the capacity calculations that the Cisco TelePresence Exchange System makes for a Meet-Me call. The table also shows the number of segments that the system reserves in cases where no media profile can be matched to the endpoint. (For more information on bridge selection based on media profiles, see the "Understanding Media Profiles and Bridge Selection" section on page B-5.)

Table B-1 Endpoint Capacity Reserved for Meet-Me Calls at Scheduling Time

Type of Call	Scenario for Determining Number of Screens	Bridge Type	Number of Segments Reserved
Provisioned Endpoint—Dial In	The system determines the number of screens (n) from the media profile of the provisioned endpoint.	CTMS	n [1,3]
		TPS (MSE 8710)	n [2]
		MSE 8510	1
Provisioned Endpoint—Dial Out	The system determines the number of screens (n) from the media profile of the provisioned endpoint.	CTMS	n [3]
		TPS (MSE 8710)	n
		MSE 8510	1
Unprovisioned Endpoint—Dial In	The system is unable to determine the number of screens, and instead uses the MeetMe Default Screens parameter (d) on the System > Global Configuration window.	CTMS	d + 1 [1]
		TPS (MSE 8710)	d [2]
		MSE 8510	1
Unprovisioned Endpoint—Dial Out	You specify a media profile for the endpoint when you configure Guest Dial Out. The number of screens (n) is based on the number of screens configured for the media profile.	CTMS	n [3]
		TPS (MSE 8710)	n
		MSE 8510	1
	You do not specify a media profile for the endpoint when you configure Guest Dial Out. The system is unable to determine the number of screens.	CTMS	2
		TPS (MSE 8710)	1
		MSE 8510	1
Remote Endpoint	The system is unable to determine the number of screens.	CTMS	4
		TPS (MSE 8710)	3
		MSE 8510	1

1. If the organization to which the endpoint belongs has Minimize Capacity unchecked, four segments are reserved on the CTMS for dial in.
2. If the organization to which the endpoint belongs has Minimize Capacity unchecked, three segments are reserved on the TPS for dial in.
3. An additional segment is reserved if the associated endpoint or media profile supports 30 FPS presentation sharing, making the total number of reserved segments n+1.

Note The Cisco TelePresence System endpoints require Software Version 1.8 in order to be supported on the Cisco TelePresence MCU MSE 8510. Three-screen H.323 endpoints are not supported on the MSE 8510.

For unprovisioned endpoints, the system will estimate a number of segments to reserve based on the bridge type if the endpoint is configured for dial in. If the endpoint is configured for Guest Dial Out, you can choose a media profile to apply to the endpoint. If you specify a media profile, the system will reserve the number of screens configured in the media profile.

The MeetMe Default Screens global setting on the System Settings > Global Configuration page allows you control over the number of segments that the system reserves for unprovisioned endpoints that do not have a media profile associated with them (in other words, for dial-in calls or for dial-out situations where no media profile is specified by the meeting scheduler). In these cases, if the meeting is hosted on a CTMS bridge, the system reserves a number of segments equal to the value MeetMe Default Screens plus one additional segment (the additional segment is to account for the possibility of 30 FPS presentation sharing). If the meeting is hosted on a TPS bridge, the system reserves a number of

segments equal to the value of MeetMe Default Screens. The system always reserves one screen for these endpoints on an MSE 8510 bridge. Note that lowering the MeetMe Default Screens value may cause capacity problems on the bridge if unprovisioned endpoints with more screens than are reserved join the meeting.

For each remote endpoint that you add to the Meet-Me meeting, the system reserves 4 segments on a CTMS, 3 segments on a TPS, or 1 segment on an MSE 8510.

You can also add additional capacity to the Meet-Me meeting by specifying a number for the Additional Capacity field. This quantity is added directly to the total capacity reserved for all the endpoints as described above.

Capacity Reservation Calculation for Rendezvous Meetings

When you create a Rendezvous meeting, you cannot add provisioned or unprovisioned endpoint participants. For this reason, the Cisco TelePresence Exchange System uses a combination of other fields on the meeting scheduling page to determine the amount of capacity to reserve for the meeting.

The combination is based on the type of bridge on which the meeting will be hosted, the value in the Number of Endpoints field, the value of MeetMe Default Screens on the System > Global Configuration window, and the value in the Additional Capacity field. For a Rendezvous meeting, the system determines the type of bridge to use based on the capabilities required by the media profile(s) that you select for the Additional Media Profiles field. (For more information on bridge selection based on media profiles, see the "Understanding Media Profiles and Bridge Selection" section on page B-5.)

The system multiplies the value that you specify for Number of Endpoints by a fixed number of segments for the type of bridge (MeetMe Default Screens + 1 for CTMS, MeetMe Default Screens for TPS, and 1 for MSE 8510). This gives a "worst-case" estimation assuming that all endpoints that join will use the same amount of bandwidth. The system then adds the value of the Additional Capacity field on to the total. For example, if you specify a value of 5 for Number of Endpoints, a value of 2 for Additional Capacity, MeetMe Default Screens is set to the default value of 3, and the meeting is hosted on CTMS, the system will reserve 5 * (3+1) + 2 = 22 segments for the meeting. Thus, if you want more fine-grained control than the "worst-case" assumption, or if you want to add capacity in a smaller multiple, you can use the Additional Capacity field.

Note At attend time, the system does not limit the actual number of endpoints that can join the Rendezvous meeting based on the Number of Endpoints field. As long as the reserved capacity is available, more endpoints can join if the endpoints have fewer screens than the "worst-case" scenario accounted for in the calculation.

Capacity Reservation and Allocation for Meet-Me and Rendezvous Meetings

The Cisco TelePresence Exchange System calculates the total capacity to reserve for a Meet-Me or Rendezvous meeting at the time you schedule or create the meeting. The point in time at which the system actually allocates the amount of resources determined by the capacity calculation for a meeting on a specific bridge depends on an additional factor for the meeting: whether the level of service of the reservation type chosen for the meeting is best-effort or guaranteed, as follows:

- Best-effort—When the first participant attempts to join the meeting, the system allocates all of the resources for the meeting.
- Guaranteed—The system allocates all of the resources for the meeting up to 15 minutes before the scheduled start of the meeting. (For a guaranteed Rendezvous meeting, the system pre-allocates the resources and does not de-allocate them unless the meeting is cancelled.)

Capacity Usage at Attend Time

When an endpoint joins a Meet-Me meeting at or after the meeting start time, or when the first participant joins a new instance of a Rendezvous meeting, the Cisco TelePresence Exchange System deducts a number of segments for the endpoint from the total reserved capacity calculated for the meeting, as shown in Table B-2.

Table B-2 Endpoint Capacity Allocated for Meet-Me Calls at Attend Time

Endpoint Type	Scenario for Determining Number of Screens	Bridge Type	Number of Segments Allocated
Provisioned	The system determines the number of screens (n) from the media profile of the provisioned endpoint.	CTMS	n + 1
		TPS (MSE 8710)	n
		MSE 8510	1
Unprovisioned or remote	The system is unable to determine the number of screens, and instead uses the MeetMe Default Screens parameter on the System > Global Configuration window (d).	CTMS	d + 1
		TPS (MSE 8710)	d
		MSE 8510	1

For example, when a provisioned one-screen endpoint joins a Meet-Me meeting at or after the meeting start time, the Cisco TelePresence Exchange System deducts two segments from the total reserved capacity calculated for the meeting if the meeting is hosted on a CTMS bridge, or one segment if the meeting is hosted on a TPS or MSE 8510. If the value of MeetMe Default Screens is set to three (the default), an unprovisioned or remote endpoint joining the meeting will cause the system to deduct 4 segments from the remaining capacity if the meeting is hosted on CTMS, three segments on TPS, or one segment on MSE 8510.

If the remaining capacity for the meeting is less than the capacity to be deducted for an endpoint that is attempting to join the meeting, the system will not allow the endpoint to join.

Capacity De-allocation

The point in time at which the Cisco TelePresence Exchange System de-allocates the resources that have been allocated for the meeting also depends on the level of service of the reservation type chosen for the meeting:

- Best-effort—When the last participant leaves the meeting, the system de-allocates the resources.
- Guaranteed—The system de-allocates the resources at the scheduled end time, regardless of whether all participants have left the meeting. For guaranteed Rendezvous meetings, the bridge resources are never de-allocated.

Understanding Media Profiles and Bridge Selection

When you provision an endpoint in the Cisco TelePresence Exchange System, you select a media profile for the endpoint. The media profile specifies the set of protocols that the endpoint supports. Each type of media bridge (CTMS, TPS or MSE 8510) supports a certain set of protocols as well.

When you invite one or more endpoints to a Meet-Me meeting, the system tries to find a common denominator between the protocols supported by the media profiles of the endpoints and the protocols supported for each bridge type. (You can also specify Additional Media Profiles so that the system takes into account the protocol capabilities required by any additional remote endpoints or unprovisioned endpoints that may dial in. Or, in the case of a Rendezvous meeting, you must specify one or more media profiles directly by using the Additional Media Profiles field so that the system can choose the correct bridge type.) In some cases, more than one bridge may have the required capabilities to host a meeting, in which case, CTX tries the bridge types sequentially in a defined order. If the first bridge type that the system tries does not have sufficient resources available, the system attempts to allocate resources from another bridge type that supports the same capabilities. The system considers CTMS resources to be the "cheapest" and MSE 8710 the most "expensive" and attempts to allocate resources from the cheapest capable bridge type first.

The system supports the following protocols for each bridge type.

Cisco TelePresence Multipoint Switch (CTMS)[1]	TIP or MUX
TPS (Cisco TelePresence Server MSE 8710)[2]	SIP, TIP, MUX, H.323, ISDN[3]
Cisco TelePresence MCU MSE 8510[2]	SIP, H.323, ISDN[3]

1. Cisco TelePresence Multipoint Switch version 1.8 required. (Version 1.8.1 is recommended.)
2. Cisco TelePresence Server version 4.2(1.50) with MSE version 4.2(1.50) required.
3. ISDN over H.323; requires Cisco TelePresence ISDN GW MSE 8321.

The system can use a mixture of protocols within a meeting on a bridge, except in the case of the CTMS, which requires that all endpoints use the same protocol (either TIP or MUX).

Table B-3 lists the types of pre-defined media profiles, the protocols supported by each, and the associated bridge selection order.

Table B-3 Pre-Defined Endpoint Media Profiles and Associated Bridge Selection Order

Endpoint/Media Profile	Screens	Supported Media Protocol(s)	Bridge Selection Order
CTS Software Release 1.8 (Native Interop) with: • CTS-500 • CTS-1000 • CTS-1100 • CTS-1300	1	MUX, TIP, SIP	CTMS, then MSE 8510, then MSE 8710
CTS Software Release 1.7 with: • CTS-500 • CTS-1000 • CTS-1100 • CTS-1300	1	MUX	CTMS, then MSE 8710
CTS Software Release 1.8 (Native Interop) with: • CTS-3000 • CTS-3200	3	MUX, TIP, SIP	CTMS, then MSE 8710

Table B-3 Pre-Defined Endpoint Media Profiles and Associated Bridge Selection Order (continued)

Endpoint/Media Profile	Screens	Supported Media Protocol(s)	Bridge Selection Order
CTS Software Release 1.7 with: • CTS-3000 • CTS-3200	3	MUX	CTMS, then MSE 8710
• Tandberg C-series • Tandberg EX-series	1	TIP, SIP, H.323	CTMS, then MSE 8510, then MSE 8710
Tandberg T3	3	H.323	MSE 8710
Generic H.323	1	H.323	MSE 8510, then MSE 8710
Generic ISDN	1	ISDN	MSE 8510, then MSE 8710
Generic SIP	1	SIP	MSE 8510, then MSE 8710

The system includes pre-defined media profiles for various endpoints, and you can add additional media profiles. For the Cisco TelePresence System endpoints, the pre-defined media profiles that correspond to CTS Release 1.8 capabilities have "(Native Interop)" in the name and description fields. If you are using CTS Release 1.7 on a Cisco TelePresence System endpoint, use the pre-defined media profile that does not have this additional text in the name.

Meet-Me Meeting Bridge Selection Example

Consider an example where only single-screen CTS endpoints using Native Interop media profiles are added to a Meet-Me meeting. In this case, the system will first try to reserve a CTMS resource for the meeting. If, however, an additional media profile is added for generic H.323, then the system will try to reserve an MSE 8510 resource. If a Tandberg T3 media profile is also added, the system will try to reserve a TPS resource.

Meet-Me Meeting Guest Dial-Out and Bridge Selection

When you schedule a Meet-Me meeting, you can specify unprovisioned endpoints and have the system dial out to add to the meeting when it starts. When you check the Guest Dial Out check box, you have the option of configuring the media profile for the endpoint.

Table B-4 lists the bridge selection order for Guest Dial Out, based on the protocol type. In this table, the media profile column refers to any selected media profile that includes the number of screens and protocols listed; for example, the first row of the table would be used if the media profile specifies one screen and supports SIP, H.323 or ISDN. If no media profile is specified, the last row in the table is used.

Table B-4 Guest Dial-Out Bridge Selection Order

Media Profile	Screens	Supported Media Protocol(s)	Bridge Selection Order
Guest Dial Out with SIP/H.323/ISDN	1	SIP, H.323, ISDN	CTMS, then MSE 8510, then MSE 8710
Guest Dial Out with SIP/H.323/ISDN	3	SIP, H.323, ISDN	MSE 8710
Guest Dial Out with TIP	1	TIP	MSE 8510, then MSE 8710

Table B-4 Guest Dial-Out Bridge Selection Order (continued)

Media Profile	Screens	Supported Media Protocol(s)	Bridge Selection Order
Guest Dial Out with TIP	3	TIP	MSE 8510, then MSE 8710
Guest Dial Out, no media profile	1	H.323	MSE 8510, then MSE 8710

Determining the Actual Bridge Type Reserved for a Meeting

You can determine the type of bridge that is hosting the meeting once the meeting has been scheduled by finding the meeting in the Collaboration Services > Meetings list, clicking on the meeting ID, and clicking the Meet-me Info tab. The Bridge Resource Type field displays the type.

Protocol Used for Dial-Out Calls At Attend Time

The protocol that the Cisco TelePresence Exchange System uses when dialing out to an endpoint depends on the bridge in use for the meeting, as follows.

Cisco TelePresence Multipoint Switch (CTMS)	TIP and MUX share a common capability negotiation mechanism, and the bridge determines the protocol to use independently. MUX is the default if the media profile of the first endpoint supports both protocols. If the media profile of an endpoint only supports one of the protocols, existing endpoints will try to renegotiate to use that protocol.
Cisco TelePresence Server MCU MSE 8510	The system attempts to dial out using a protocol that is supported by the media profile of the endpoint. If more than one protocol is specified in the media profile, the system tries a supported protocol in the following order: H.323, SIP, ISDN. For example, for an endpoint with a media profile that supports SIP and ISDN, the system would first attempt to dial out by using SIP.
Cisco TelePresence Server MSE 8710	The system attempts to dial out using a protocol that is supported by the media profile of the endpoint. If more than one protocol is specified in the media profile, the system tries a supported protocol in the following order: H.323, TIP, MUX, SIP, ISDN. For example, for an endpoint with a media profile that supports SIP and ISDN, the system would first attempt to dial out by using SIP.

Protocol Used for Dial-In Calls At Attend Time

The protocol that the Cisco TelePresence Exchange System uses when an endpoint dials in also depends on the bridge in use for the meeting, as follows. (H.323 and ISDN are not supported for dial-in.)

Cisco TelePresence Multipoint Switch (CTMS)	TIP and MUX share a common capability negotiation mechanism, so the bridge determines the protocol to use independently. MUX is the default if the first endpoint supports both protocols. If an endpoint only supports one of the protocols, that protocol is used, and existing endpoints will try to renegotiate to use this protocol.
Cisco TelePresence Server MCU MSE 8510	The Cisco TelePresence Exchange System only supports SIP for dial-in with the MSE 8510, so this protocol is always chosen.
Cisco TelePresence Server MSE 8710	The Cisco TelePresence Exchange System checks to see if the endpoint that is dialing in is provisioned for the meeting. If so, and if the endpoint supports MUX or TIP, the bridge will negotiate one of these two protocols. If the endpoint is unprovisioned, the system checks the route the endpoint dialed in on. If the Endpoint Type for this route is set to CTS, the bridge will negotiate MUX or TIP. Otherwise, the bridge will attempt to negotiate SIP, MUX or TIP. (Endpoints running CTS 1.7 and earlier versions do not have the capability to negotiate between SIP and MUX or TIP, so if the Endpoint Type for the route is set to BOTH or INTEROP, the call will fail for these endpoints.)

APPENDIX C

Command Reference

This appendix describes the CLI commands that are supported on the Cisco TelePresence Exchange System:

file dump

To display the contents of one or more files on the screen, one page at a time, enter the following command.

file dump {**activelog | inactivelog | install**} *file-spec* [**recent**]

Syntax Description

activelog	Displays the contents of one or more files that are in the currently active partition.
inactivelog	Displays the contents of one or more files that are in the inactive partition, which, if the system had been upgraded, contains the previous version of the software and the logs from before the most recent upgrade.
install	Displays the contents of one or more log files that are related to installation.
file-spec	File or files you want to dump onto the screen. You can use an asterisk (*) as a wildcard. Enter the *file-spec* as one of the following items: • Directory • Filename • Directory path and filename
recent	(Optional) Displays the content of the most recently changed file in the directory.

Usage Guidelines

If you specify multiple files in the *file-spec*, this command concatenates, or joins, the files and then displays the contents on the screen, one page at a time.

Examples

The following example shows how to display the contents of one file that is in the active partition:

```
admin: file dump activelog ctc/log/server.log
2011-03-16 21:03:01,123 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
JBossTS Transaction Service (JTA version) - JBoss Inc.
2011-03-16 21:03:01,124 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
Setting up property manager MBean and JMX layer
2011-03-16 21:03:01,236 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
Starting recovery manager
2011-03-16 21:03:01,293 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
Recovery manager started
2011-03-16 21:03:01,293 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
Binding TransactionManager JNDI Reference
2011-03-16 21:03:06,245 INFO  [org.jboss.cache.TreeCache] viewAccepted():
[10.22.140.75:32774|0] [10.22.140.75:32774]
2011-03-16 21:03:06,257 INFO  [org.jboss.cache.TreeCache] TreeCache local address is
10.22.140.75:32774
2011-03-16 21:03:06,257 INFO  [org.jboss.cache.TreeCache] State could not be retrieved (we
are the first member in group)
2011-03-16 21:03:06,257 INFO  [org.jboss.cache.TreeCache] parseConfig(): PojoCacheConfig
is empty
2011-03-16 21:03:07,070 INFO  [org.jboss.wsf.stack.jbws.NativeServerConfig] JBoss Web
Services - Native
2011-03-16 21:03:07,070 INFO  [org.jboss.wsf.stack.jbws.NativeServerConfig]
```

```
jbossws-native-2.0.1.SP2_CP08 (build=201003171618)
2011-03-16 21:03:07,474 INFO  [org.jboss.jmx.adaptor.snmp.agent.SnmpAgentService] SNMP
agent going active
2011-03-16 21:03:07,629 INFO
[org.jboss.ha.framework.interfaces.HAPartition.Partition-139-230] Initializing
```

Related Commands

Command	Description
file get	Retrieves files by using SSH file transfer protocol (SFTP).
file list	Lists the files and subdirectories that are in a specified directory.
file search	Searches the content of log files and displays the lines that match a specified regular expression.
file tail	Displays the last several lines of a file on the screen and displays appended data as the file grows.
file view	Displays the contents of a file.

file get

To retrieve files by using SSH file transfer protocol (SFTP), enter the following command.

file get {**activelog | backup | inactivelog | install**} *file-spec* [**reltime** *reltime-age* **| abstime** *abstime-start abstime-end* **| match** *regex* **| recurs**]

Syntax Description

activelog	Gets log files from the currently active partition.
backup	Gets files from the backup partition.
inactivelog	Gets log files from the inactive partition, which, if the system had been upgraded, contains the previous version of the software and the logs from before the most recent upgrade.
install	Gets log files that are related to installation.
file-spec	File or files you want to get through SFTP. You can use an asterisk (*) as a wildcard. Enter the *file-spec* as one of the following items: • Directory • Filename • Directory path and filename
reltime	(Optional) Gets files that are no older than the specified *reltime-age*.
reltime-age	How recently files must have been updated in order to include them in the get operation. Enter the *reltime-age* as follows, where you specify the units and then the value: {**months	weeks	days	hours	minutes**} *number*
abstime	(Optional) Gets files that have been updated between the absolute times *abstime-start* and *abstime-end*.
abstime-start	Enter the *abstime-start* and the *abstime-end* as *hh***:***mm***:***MM***/***DD***/***YY*, to specify the hour, minute, month, day, and year.
abstime-end	
match	(Optional) Gets files whose filenames contain characters that match a regular expression.
regex	Regular expression for which you want to find matches in the filenames.
recurs	(Optional) Gets all files, including the subdirectories, of a specified directory.

Usage Guidelines

When you enter the command, you are prompted to enter the IP address, username, and password for the SFTP server.

Examples

The following example shows how to get all log files that may be of interest to a customer support representative:

```
admin: file get activelog ctc/log/*.log
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 5
```

```
Total size in Bytes: 180218286
Total size in Kbytes: 175994.42
Would you like to proceed [y/n]? y
SFTP server IP: 10.22.140.75
SFTP server port [22]:
User ID: root
Password: ********

Download directory: /tmp

.....
Transfer completed.
:
```

Related Commands

Command	Description
file dump	Displays the contents of one or more files on the screen, one page at a time.
file list	Lists the files and subdirectories that are in a specified directory.
file search	Searches the content of log files and displays the lines that match a specified regular expression.
file tail	Displays the last several lines of a file on the screen and displays appended data as the file grows.
file view	Displays the contents of a file.

file list

To list the files and subdirectories in a directory, enter the following command.

file list {**activelog** | **backup** | **inactivelog** | **install**} *file-spec* [**page**] [**detail**] [**reverse**] [**date**] [**size**]

Syntax Description

activelog	Specifies the currently active partition.
backup	Specifies the backup partition.
inactivelog	Specifies the inactive partition, which, if the system had been upgraded, contains the previous version of the software and the logs from before the most recent upgrade.
install	Specifies the install partition.
file-spec	Directory whose files and subdirectories you want to list. You can use an asterisk (*) as a wildcard.
page	(Optional) Displays the output one screen at a time.
detail	(Optional) Includes the details of each file and subdirectory in the list.
reverse	(Optional) Displays the list in the reverse sort order.
date	(Optional) Sorts the list items by date.
size	(Optional) Sorts the list items by file size.

Examples

The following example shows how to list all active log files in a specified directory:

```
admin: file list activelog ctc/log/cisco/*
ctc-engine-crm.log                      ctc-engine-hibernate.log
ctc-engine-initapp.log                  ctc-engine-interop-tps.log
ctc-engine-ivr.log                      ctc-engine-license.log
ctc-engine-meetme.log                   ctc-engine-netop.log
ctc-engine-ns.log                       ctc-engine-servicecontrol.log
ctc-engine-spring.log                   ctc-engine.log
dir count = 0, file count = 12
```

Related Commands

Command	Description
file dump	Displays the contents of one or more files on the screen, one page at a time.
file get	Retrieves files by using SSH file transfer protocol (SFTP).
file search	Searches the content of log files and displays the lines that match a specified regular expression.
file tail	Displays the last several lines of a file on the screen and displays appended data as the file grows.
file view	Displays the contents of a file.

file search

To search the content of log files and display the lines that match a specified regular expression, enter the following command.

file search {**activelog** | **inactivelog** | **install**} *file-spec reg-exp* [**reltime** *reltime-age* | **abstime** *abstime-start abstime-end*] [**ignorecase**] [**recurs**]

Syntax Description

activelog	Searches the log files that are in the currently active partition.
inactivelog	Searches the log files that are in the inactive partition, which, if the system had been upgraded, contains the previous version of the software and the logs from before the most recent upgrade.
install	Searches the installation log files.
file-spec	Directories or files to search. You can use an asterisk (*) as a wildcard. Enter the *file-spec* as one of the following items: • Directory • Filename • Directory path and filename
reg-exp	Regular expression against which you want to find matches in the content of the file or files.
reltime	(Optional) Gets files that are no older than the specified *reltime-age*.
reltime-age	How recently files must have been updated in order to include them in the get operation. Enter the *reltime-age* as follows, where you specify the units and then the value: {**days** | **hours** | **minutes**} *number*
abstime	(Optional) Searches files that have been created or updated between the absolute times *abstime-start* and *abstime-date*.
abstime-start	Enter the *abstime-start* and *abstime-date* as *hh***:***mm***:***ss MM***/***DD***/***YY*, to specify the hour, minute, second, month, day, and year.
abstime-end	
ignorecase	(Optional) Ignores the case of characters in the regular expression while searching for the files.
recurs	(Optional) Searches all files, including the subdirectories, of a specified directory.

Usage Guidelines

The output is displayed one page at a time. If the search term is found in only one file, the filename appears at the top of the output. If the search term is found in multiple files, each line of the output begins with the filename in which the matching line was found.

Examples

The following example shows how to search active platform log files for errors:

```
admin: file search activelog platform/log/* Err[a-z] ignorecase

Searching path: /var/log/active/platform/log/*
/var/log/active/platform/log/cli00028.log:2011-03-06 00:33:10,266 INFO [main] -
fileError=(disk_full=false)
```

```
/var/log/active/platform/log/cli00028.log:2011-03-06 00:33:10,266 INFO [main] -
fileError=(inode_full=false)
/var/log/active/platform/log/cli00028.log:2011-03-06 00:33:10,266 INFO [main] -
fileError=(no_write=false)
/var/log/active/platform/log/cli00028.log:2011-03-06 00:33:10,266 INFO [main] -
fileError=(internal_error=false)
/var/log/active/platform/log/clustermgr00000002.log:01:34:20.266 |       clm_error_code(0)
/var/log/active/platform/log/clustermgr00000002.log:01:34:20.266 |connectivity test error
code set to 0
…
Search completed
```

Related Commands

Command	Description
file dump	Displays the contents of one or more files on the screen, one page at a time.
file get	Retrieves files by using SSH file transfer protocol (SFTP).
file list	Lists the files and subdirectories that are in a specified directory.
file tail	Displays the last several lines of a file on the screen and displays appended data as the file grows.
file view	Displays the contents of a file.

file tail

To display the last several lines of a file on the screen and continue to display appended data as the file grows, enter the following command.

file tail {**activelog | inactivelog | install**} *file-spec* [*num-lines*] [**recent**]

Syntax Description

activelog	Specifies a file that is in the currently active partition.
inactivelog	Specifies a file that is in the inactive partition, which, if the system had been upgraded, contains the previous version of the software and the logs from before the most recent upgrade.
install	Specifies an installation-related log file.
file-spec	File to display the last several lines of, and any appended data as the file grows. You can use an asterisk (*) as a wildcard. Enter the *file-spec* as one of the following items: • Filename • Directory path and filename • Directory—If you enter only a directory, you need to specify the file by adding the **recent** keyword.
num-lines	(Optional) Number of lines to display in the output. Default: 10.
recent	(Optional) Specifies the most recently changed file in the directory.

Usage Guidelines

Use this command when you want to quickly display the most recent entries in a log file and display any additional logs as they are written into the file.

Examples

The following example shows how to display the tail end of a file:

```
admin: file tail activelog ctc/log/cisco/ctc-engine.log
2011-03-17 04:13:10,717 DEBUG {ctx-eng-2||}-[DataAccessor:getAllOnlineResources|273] -
Online Resources:[]
2011-03-17 04:13:25,716 INFO  {ctx-eng-2||}-[MeetmeOperation:timeout|274] - Updating
current resources list from database
2011-03-17 04:13:25,716 DEBUG {ctx-eng-2||}-[DataAccessor:getAllOfflineResources|112] -
ivrResourcesList :[]
2011-03-17 04:13:25,716 DEBUG {ctx-eng-2||}-[DataAccessor:getAllOfflineResources|125] -
ctmsResourcesList :[]
2011-03-17 04:13:25,716 DEBUG {ctx-eng-2||}-[DataAccessor:getAllOfflineResources|138] -
cuvmResourceList :[]
2011-03-17 04:13:25,716 DEBUG {ctx-eng-2||}-[DataAccessor:getAllOfflineResources|151] -
sipResourceList :[]
2011-03-17 04:13:25,717 DEBUG {ctx-eng-2||}-[DataAccessor:getAllOfflineResources|164] -
tpsResourceList :[]
2011-03-17 04:13:25,717 DEBUG {ctx-eng-2||}-[DataAccessor:getAllOfflineResources|177] -
media2ResourceList :[]
2011-03-17 04:13:25,717 DEBUG {ctx-eng-2||}-[DataAccessor:getAllOfflineResources|189] -
Offline Resources:[]
2011-03-17 04:13:25,717 DEBUG {ctx-eng-2||}-[DataAccessor:getAllOnlineResources|273] -
Online Resources:[]
2011-03-17 04:13:40,716 INFO  {ctx-eng-2||}-[MeetmeOperation:timeout|274] - Updating
current resources list from database
```

Related Commands

Command	Description
file dump	Displays the contents of one or more files on the screen, one page at a time.
file get	Retrieves files by using SSH file transfer protocol (SFTP).
file list	Lists the files and subdirectories that are in a specified directory.
file search	Searches the content of log files and displays the lines that match a specified regular expression.
file view	Displays the contents of a file.

file view

To display the contents of a file, enter the following command.

file view {**activelog | inactivelog | install**} *file-spec*

Syntax Description

activelog	Displays the contents of a file in the currently active partition.
inactivelog	Displays the contents of a file in the inactive partition, which, if the system had been upgraded, contains the previous version of the software and the logs from before the most recent upgrade.
install	Displays the contents of an installation-related log file.
file-spec	File you want to view. You can use an asterisk (*) as a wildcard as long as it resolves to a single file. Enter the *file-spec* as a filename or as a directory path with a filename.

Usage Guidelines

If the command output spans multiple screens, use the options that appear at the bottom of the screen to navigate within the file contents or to quit the view.

Examples

The following example shows how to display the contents of a file:

```
admin: file view activelog ctc/log/server.log

2011-03-23 20:51:44,859 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
JBossTS Transaction Service (JTA version) - JBoss Inc.
2011-03-23 20:51:44,861 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
Setting up property manager MBean and JMX layer
2011-03-23 20:51:44,987 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
Starting recovery manager
2011-03-23 20:51:45,042 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
Recovery manager started
2011-03-23 20:51:45,042 INFO  [com.arjuna.ats.jbossatx.jta.TransactionManagerService]
Binding TransactionManager JNDI Reference
2011-03-23 20:51:49,857 INFO  [org.jboss.cache.TreeCache] viewAccepted():
[10.22.139.125:33935|0] [10.22.139.125:33935]
2011-03-23 20:51:49,871 INFO  [org.jboss.cache.TreeCache] TreeCache local address is
10.22.139.125:33935
2011-03-23 20:51:49,871 INFO  [org.jboss.cache.TreeCache] State could not be retrieved (we
are the first member in group)
2011-03-23 20:51:49,871 INFO  [org.jboss.cache.TreeCache] parseConfig(): PojoCacheConfig
is empty
2011-03-23 20:51:50,680 INFO  [org.jboss.wsf.stack.jbws.NativeServerConfig] JBoss Web
Services - Native
2011-03-23 20:51:50,680 INFO  [org.jboss.wsf.stack.jbws.NativeServerConfig]
jbossws-native-2.0.1.SP2_CP09 (build=201011082206)
2011-03-23 20:51:51,105 INFO  [org.jboss.jmx.adaptor.snmp.agent.SnmpAgentService] SNMP
agent going active
2011-03-23 20:51:51,279 INFO
[org.jboss.ha.framework.interfaces.HAPartition.Partition-139-90] Initializing
2011-03-23 20:51:53,329 INFO
[org.jboss.ha.framework.interfaces.HAPartition.Partition-139-90] Number of cluster
members: 1
2011-03-23 20:51:53,329 INFO
[org.jboss.ha.framework.interfaces.HAPartition.Partition-139-90] Other members: 0
```

```
2011-03-23 20:51:53,329 INFO
[org.jboss.ha.framework.interfaces.HAPartition.Partition-139-90] Fetching state (will wait
for 30000 milliseconds):
2011-03-23 20:51:53,329 INFO
[org.jboss.ha.framework.interfaces.HAPartition.Partition-139-90] State could not be
retrieved (we are the first member in group)
2011-03-23 20:51:53,347 INFO  [org.jboss.ha.jndi.HANamingService] Started ha-jndi
bootstrap jnpPort=1100, backlog=50, bindAddress=/0.0.0.0
2011-03-23 20:51:53,426 INFO  [org.jboss.cache.TreeCache] No transaction manager lookup
class has been defined. Transactions cannot be used
2011-03-23 20:51:55,527 INFO  [org.jboss.cache.TreeCache] viewAccepted():
[10.22.139.125:33940|0] [10.22.139.125:33940]

options: q=quit, n=next, p=prev, b=begin, e=end (lines 1 - 20 of 952) :
…
```

Related Commands

Command	Description
file dump	Displays the contents of one or more files on the screen, one page at a time.
file get	Retrieves files by using SSH file transfer protocol (SFTP).
file list	Lists the files and subdirectories that are in a specified directory.
file search	Searches the content of log files and displays the lines that match a specified regular expression.
file tail	Displays the last several lines of a file on the screen and displays appended data as the file grows.

set adminserver changedbip

To change the database server virtual IP (VIP) address that is configured on the administration server, enter the following command.

set adminserver changedbip *database-vip-address*

Syntax Description

database-vip-address	VIP address of the database servers.

Usage Guidelines

Use this command only on the administration server.

The VIP address that is shared by the database servers is entered during the installation of the administration server. If the database server VIP address was entered incorrectly, use this command to correct the configuration.

After you use this command to change the database server VIP address, you need to restart the administration server by entering the utils service adminserver stop and utils service adminserver start commands.

Examples

The following example shows how to change the database VIP address on the administration server:

```
admin: set adminserver changedbip 10.22.128.234
Database server IP address has been changed to 10.22.128.234
Please restart the Admin server using the 'utils service adminserver stop|start' command
for the change to take effect
```

Related Commands

Command	Description
show dbip	Displays the database VIP address that is defined on the administration server or call engine server.
set sipserver changedbip	Configures the database VIP address that is configured on the call engine server.

set adminserver trapvip

To add or remove a virtual IP (VIP) address in product-specific SNMP notifications, enter the following command.

set adminserver trapvip {**ena** *vip-address* | **dis**}

Syntax Description

ena	Adds the VIP address to product-specific notifications.
vip-address	VIP address that your remote management system can use to identify a specific Cisco TelePresence Exchange System server cluster. For a list of VIP address options, see the "Adding a Cluster-Identifying VIP Address to SNMP Notifications" section on page 26-8.
dis	Removes the VIP address from product-specific notifications.

Usage Guidelines

Use this command only on the administration server.

For details, see the "Adding a Cluster-Identifying VIP Address to SNMP Notifications" section on page 26-8.

Examples

The following example shows how to add a VIP address to product-specific notifications:

```
admin: set adminserver trapvip ena 10.22.128.212
Updated SNMP Trap VIP to 10.22.128.212

admin: show trapvip
SNMP Trap VIP: 10.22.128.212
```

The following example shows how to remove the VIP address from product-specific notifications:

```
admin: set adminserver trapvip dis
Disabled SNMP Trap VIP

admin: show trapvip
SNMP Trap VIP is not enabled/configured on this server.
```

Related Commands

Command	Description
show trapvip	Displays the VIP address, if configured, in product-specific SNMP notifications.
set snmp trapdest add	Adds an SNMP trap destination.

set cdp disable

To disable CDP for one or all interfaces on a server, enter the following command.

set cdp disable {*interface* | **all**}

Syntax Description

interface	Interface on which you want to disable CDP.
all	Specifies that you want to disable CDP on all interfaces of the server.

Usage Guidelines

To list the interfaces on which CDP is enabled, use the **show cdp config** command. To specify a particular interface for which you want to disable CDP, enter the interface name as it appears in the **show cdp config** command output.

To list the interfaces that would be affected if you entered **set cdp disable all**, use the **show cdp list** command.

Examples

The following example shows how to display the CDP-enabled interfaces on a database server and how to disable CDP for one of those interfaces:

```
admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 60 seconds
    Hold Time   : 180 seconds
    Enabled on  : bond1
    Enabled on  : bond0

admin: set cdp disable bond1
CDP configuration updated.
cdp.....................Stopped
cdp............................Starting - PID <18427>
admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 60 seconds
    Hold Time   : 180 seconds
    Enabled on  : bond0
```

Related Commands

Command	Description
set cdp enable	Enables CDP for one or all interfaces on a server.
show cdp	Displays CDP information for a server.

set cdp enable

To enable CDP for one or all interfaces on a server, enter the following command.

set cdp enable {*interface* | **all**}

Syntax Description

interface	Interface on which you want to enable CDP.
all	Specifies that you want to enable CDP on all interfaces of the server.

Usage Guidelines

By default, CDP is enabled on the Bond 0 interface on each Cisco TelePresence Exchange System server.

To list the interfaces on which CDP is enabled, use the **show cdp config** command. To list all available interfaces on which you can enable CDP, use the **show cdp list** command.

To specify a particular interface for which you want to enable CDP, enter the interface name as it appears in the **show cdp list** command output. The **show cdp list** command output lists the interfaces that would be affected if you entered **set cdp enable all**.

Examples

The following example shows how to display the CDP-enabled interfaces on a database server, how to view all interfaces on which you may enable CDP, and how to enable CDP for all those interfaces:

```
admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 60 seconds
    Hold Time   : 180 seconds
    Enabled on  : bond0

admin: show cdp list
  Available Interfaces:
     bond0
     bond1

admin: set cdp enable all
  Enabled Interfaces:
     bond0
     bond1
CDP configuration updated.
cdp.....................Stopped
cdp.........................Starting - PID <22634>

admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 60 seconds
    Hold Time   : 180 seconds
    Enabled on  : bond1
    Enabled on  : bond0
```

Related Commands

Command	Description
set cdp disable	Disables CDP for one or all interfaces on a server.
show cdp	Displays CDP information for a server.

set cdp holdtime

To specify the length of time that the receiving device should hold a CDP packet from this server before discarding it, enter the following command.

set cdp holdtime *seconds*

Syntax Description

seconds	Hold time, in seconds, to be sent in the CDP update packets. Default: 180.

Usage Guidelines

CDP packets are sent with a time to live, or hold time, value. The receiving device will discard the CDP information in the CDP packet after the hold time has elapsed.

You can set the hold time to a value lower than the default setting of 180 seconds if you want the receiving devices to update their CDP information more frequently.

The CDP hold time must be set to a higher number of seconds than the time between CDP transmissions, which is set by using the **set cdp timer** command.

Examples

The following example shows how to display the current CDP hold time value, how to change the value, and how to verify the new value:

```
admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 60 seconds
    Hold Time   : 180 seconds
    Enabled on  : bond0

admin: set cdp holdtime 120
CDP configuration updated.
cdp.....................Stopped
cdp...........................Starting - PID <16598>

admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 60 seconds
    Hold Time   : 120 seconds
    Enabled on  : bond0
```

Related Commands

Command	Description
show cdp	Displays CDP information for a server.
set cdp timer	Specifies how often the server sends CDP updates.

set cdp timer

To specify how often the server sends CDP updates, enter the following command.

set cdp timer *seconds*

Syntax Description

seconds	Server sends CDP update packets, in seconds. Default: 60.

Usage Guidelines

Verify that you set a timer value that is lower than the CDP hold time, which you configure via the **set cdp holdtime** command. Otherwise, the receiving devices will discard the CDP information from this server before the server sends the next update.

If you want the neighboring devices to receive more frequent updates from this server, change the CDP timer value to a lower number. If, however, you want to reduce the network bandwidth utilization, change the CDP timer value to a higher number.

Examples

The following example shows how to display the current CDP timer value, how to change the value, and how to verify the new value:

```
admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 60 seconds
    Hold Time   : 120 seconds
    Enabled on  : bond0

admin: set cdp timer 90
CDP configuration updated.
cdp.....................Stopped
cdp.........................Starting - PID <27387>

admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 90 seconds
    Hold Time   : 120 seconds
    Enabled on  : bond0
```

Related Commands

Command	Description
show cdp	Displays CDP information for a server.
set cdp holdtime	Specifies the length of time that the receiving device should hold a CDP packet from this server before discarding it.

set network failover dis

To disable NIC teaming, enter the following command.

set network failover dis

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

The Cisco TelePresence Exchange System software implements NIC teaming to bond certain interfaces together for redundancy:

Server	Bonded Interfaces
Database server	Bond 0—Ethernet 0 with Ethernet 2 Bond 1—Ethernet 1 with Ethernet 3
Administration server	Bond 0—Ethernet 0 with Ethernet 1
Call engine server	Bond 0—Ethernet 0 with Ethernet 1

Use this command to remove the bond on an administration or call engine server, for example, when you need to change the IP address of the server.

Note This command is not supported on the database servers. Cisco does not support changing the IP addresses or virtual IP (VIP) address of the database servers. You can change the IP and VIP addresses only by reinstalling the database servers.

Caution Entering this command will cause temporary loss of connectivity to the server. Cisco recommends that you use this command only during maintenance windows.

Examples

The following example shows how to disable NIC teaming on the server:

```
admin: set network failover dis
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?

Enter "yes" to continue or any other key to abort:

yes
executing ...
```

Related Commands

Command	Description
set network failover ena	Enables the bond between Ethernet 0 and Ethernet 1 on the administration server or call engine server.
show network failover	Displays which interfaces are bonded together on the server.

set network failover ena

To enable NIC teaming on an administration or call engine server, enter the following command.

set network failover ena

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

If NIC teaming was previously disabled on an administration or call engine server, use this command to reenable NIC teaming. When entered, the Cisco TelePresence Exchange System software bonds Ethernet 0 with Ethernet 1 together for redundancy as Bond 0.

Caution Entering this command will cause temporary loss of connectivity to the server. Cisco recommends that you use this command only during maintenance windows.

Examples

The following example shows how to enable NIC teaming:

```
admin: set network failover ena
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?

Enter "yes" to continue or any other key to abort:

yes
executing ...
```

Related Commands

Command	Description
set network failover dis	Disables the bond between Ethernet 0 and Ethernet 1 on the administration server or call engine server.
show network failover	Displays which interfaces are bonded together on the server.

set network gateway

To change the default gateway for a server, enter the following command.

set network gateway *ip-address*

Syntax Description

ip-address	IP address of the default gateway.

Usage Guidelines

Typically, the default gateway is configured only during server installation. Use this command to change or correct the configuration after installation, for example, if you move a server into a different network.

Caution Entering this command will cause temporary loss of connectivity to the server. Cisco recommends that you use this command only during maintenance windows.

Examples

The following example shows how to configure the default gateway:

```
admin: set network gateway 10.22.139.97
     ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity


Continue (y/n)? y
admin:
```

Related Commands

Command	Description
set network ip eth0	Configures the IP address of the server.

set network ip eth0

To change the IP address of a server, enter the following command.

set network ip eth0 *ip-address subnet-mask*

Syntax Description

ip-address	IP address of the server.
subnet-mask	Subnet mask.

Usage Guidelines

Typically, the IP address is configured only during server installation. Use this command to change or correct the configuration after installation.

Note Cisco does not support changing the IP addresses or virtual IP (VIP) address of the database servers. You can change the IP and VIP addresses only by reinstalling the database servers.

You will need to disable NIC teaming on the server before you can use this command. For details, see the "Changing the IP Address of an Administration or Call Engine Server" section on page 28-1.

Caution Entering this command will cause the system to restart. Cisco recommends that you use this command only during maintenance windows.

Examples

The following example shows how to change the IP address of the server:

```
admin: set network ip eth0 10.22.139.106 255.255.255.240
          ***   W A R N I N G   ***
The system will be rebooted after the change.


Continue (y/n)? y
SIP server listening address has been changed to 10.22.139.106
Please restart the SIP server using the 'utils service sipserver stop|start' command for
the change to take effect


Warning: Restart could take up to 5 minutes...
Shutting down Service Manager will take some time..
\   Service Manager shutting down services... Please Wait
DONE!!!!

Broadcast message from root (Thu Feb 17 23:58:48 2011):

The system is going down for reboot NOW!

Restart has succeeded
```

Related Commands

Command	Description
show network eth0	Displays information about the Ethernet 0 interface on the server.
set network failover dis	Disables NIC teaming and removes bonds between the Ethernet interfaces.

set password admin

To change the administrator password for accessing the CLI, enter the following command.

set password admin

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

The new password must be at least 6 characters long and cannot repeat a previously used password. The password should not be a word that can be found in a dictionary, any variation of the administrator username, or any name.

You must use the same administrator username and password on all Cisco TelePresence Exchange System servers, because the administration servers also use the administrator credentials over SSH to get the status of all nodes in the server cluster.

Examples

The following example shows how to change the administrator password:

```
admin: set password admin
   Please enter the old password: ********
   Please enter the new password: *********
Reenter new password to confirm: *********
Please wait...

Password updated successfully.
```

Related Commands

None.

set sipserver changedbip

To change the database server virtual IP (VIP) address that is configured on the call engine server, enter the following command.

set sipserver changedbip *database-vip-address*

Syntax Description

database-vip-address	VIP address of the database servers.

Usage Guidelines

Use this command only on the call engine server.

The VIP address that is shared by the database servers is entered during the installation of the call engine server. If the database server VIP address was entered incorrectly, use this command to correct the configuration.

After you use this command to change the database server VIP address, you need to restart the call engine server by entering the utils service sipserver stop and utils service sipserver start commands.

Examples

The following example shows how to change the database VIP address on the call engine server:

```
admin: set sipserver changedbip 10.22.140.184
Database server IP address has been changed to 10.22.140.184
Please restart the SIP server using the 'utils service sipserver stop|start' command for
the change to take effect
```

Related Commands

Command	Description
show dbip	Displays the database VIP address that is defined on the administration server or call engine server.
set adminserver changedbip	Configures the database VIP address that is configured on the administration server.

set sipserver siplb dis

To remove the SIP load balancer virtual IP (VIP) address and port configuration on the call engine servers, enter the following command.

set sipserver siplb dis

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command only on the call engine servers.

Note Changes take effect only after you restart the SIP server by using the **utils service sipserver stop** and **utils service sipserver start** commands.

Examples

The following example shows how to remove the SIP load balancer VIP address and port configuration:

```
admin: set sipserver siplb dis
SIP Loadbalancing has been disabled.
Please restart the SIP server using the 'utils service sipserver stop|start' command for
the change to take effect
```

Related Commands

Command	Description
set sipserver siplb ena	Configures the SIP load balancer VIP address and port on the call engine server.
show siplb	Displays the configured SIP load balancer VIP address and port.

set sipserver siplb ena

To configure the virtual IP (VIP) address and port number of the SIP load balancer, which is the Cisco Application Control Engine (ACE), enter the following command.

set sipserver siplb ena *load-balancer-vip-address* [*port*]

Syntax Description

load-balancer-vip-address	VIP address of the SIP load balancer.
port	(Optional) Port number on which the call engine connects to the SIP load balancer. Default: 5060.

Usage Guidelines

Use this command only on the call engine servers.

Typically, the VIP address and port of the SIP load balancer are configured only during the installation of the call engine servers. Nevertheless, this command enables you to set or modify the SIP load balancer VIP address and port after installation.

Note Changes take effect only after you restart the call engine server by using the **utils service sipserver stop** and **utils service sipserver start** commands.

Examples

In the following example, the SIP load balancer VIP address is defined as 192.0.2.25. Because the port number is not specified, the default port 5060 is used.

```
admin: set sipserver siplb ena 192.0.2.25
SIP Loadbalancing is not configured on this engine.
SIP Load Balancer address has been changed to 192.0.2.25
SIP Load Balancer port has been changed to 5060
Please restart the SIP server using the 'utils service sipserver stop|start' command for
the change to take effect
```

Related Commands

Command	Description
show siplb	Displays the configured SIP load balancer VIP address and port.
set sipserver siplb dis	Removes the SIP load balancer VIP address and port configuration on the call engine server.

set snmp trapdest add

To add an SNMP trap destination, enter one of the following commands, depending on whether you are using SNMP version 3 or 2c.

set snmp trapdest add 3 *username destination*[**:***port*] [*level*] *passphrase* [*engineID*]

set snmp trapdest add 2c *community-string destination*[**:***port*] [*passphrase*]

Syntax Description

3	Specifies SNMP version 3.
username	SNMP username.
2c	Specifies SNMP version 2c.
community-string	Community string.
destination	IP address or hostname of the host to which the system sends the trap notifications.
port	(Optional) Port number. Default: 162.
level	(Optional) Enter one of the following values: • **authNoPriv**—(Default) Authenticates packets based on the HMAC-MD5 algorithm with no encryption. • **authPriv**—Authenticates packets based on the HMAC-MD5 algorithm with DES encryption. • **noauthNoPriv**—Does not authenticate or encrypt packets.
passphrase	(Optional for SNMP version 2c) User password.
engineID	(Optional) Engine ID to use for the trap. By default, the system engine ID is used.

Usage Guidelines

Use this command on each Cisco TelePresence Exchange System server from which you want to receive trap notifications. For details, see the "Adding SNMP Trap Destinations" section on page 26-6.

Examples

The following example shows how to add a trap destination by using SNMP version 2c:

```
admin: set snmp trapdest add 2c public 10.93.231.187
Successfully added trap destination
```

Related Commands

Command	Description
show snmp trapdests	Displays the configured SNMP trap destinations.
set snmp trapdest del	Deletes an SNMP trap destination.

set snmp trapdest del

To delete an SNMP trap destination, enter the following command.

set snmp trapdest del

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

When you use this command, you will see a list of SNMP trap destinations that are configured on the server. You will then be prompted to choose which trap destination to delete from the list.

For details, see the "Removing an SNMP Trap Destination" section on page 26-7.

Examples

The following example shows that the second SNMP trap destination is deleted:

```
admin: set snmp trapdest del
  1) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = TimTrap               PW   = authpriv
           Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  2) Host = 10.101.180.49 (Version 3)

     Version 3 Options:
            User = TimTrap2              PW   = authpriv
           Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  3) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = trapusr               PW   = trappass
           Level = authnopriv            Hash = md5
        EngineID = 0x8000DEECAFE8111BEEFADE


  Enter which trap number to delete: 2
Successfully deleted trap destination
```

The following show command verifies the removal of the specified SNMP trap destination:

```
admin: show snmp trapdests
  1) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = TimTrap               PW   = authpriv
           Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  2) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = trapusr               PW   = trappass
           Level = authnopriv            Hash = md5
        EngineID = 0x8000DEECAFE8111BEEFADE
```

Related Commands

Command	Description
show snmp trapdests	Displays the configured SNMP trap destinations.
set snmp trapdest add	Adds an SNMP trap destination.

set snmp user add

To add an SNMP user, enter one of the following commands, depending on whether you are using SNMP version 3 or 2c.

set snmp user add 3 *snmp-username access* [*level*] *passphrase*

set snmp user add 2c *community-string access* [*passphrase*]

Syntax Description

3	Specifies SNMP version 3.
snmp-username	SNMP username.
2c	Specifies SNMP version 2c.
community-string	Community string.
access	Enter one of the following values: • **r**—Read access. • **w**—Write access. • **rw**—Read and write access.
level	(Optional for SNMP version 2c) Enter one of the following values: • **authNoPriv**—(Default) Authenticates packets based on the HMAC-MD5 algorithm with no encryption. • **authPriv**—Authenticates packets based on the HMAC-MD5 algorithm with DES encryption. • **noauthNoPriv**—Uses a username match for authentication.
passphrase	(Optional for noauthNoPriv level or SNMP version 2c) User password.

Usage Guidelines

If you use both SNMP versions 3 and 2c, verify that no SNMP usernames are the same as any community strings.

For details, see the "Adding SNMP Users" section on page 26-4.

Examples

The following example shows how to add a user using SNMP version 2c:

```
admin: set snmp user add 2c public r
Successfully added user
```

The following example shows how to add a user using SNMP version 3:

```
admin: set snmp user add 3 test rw authpriv tstpwd
Successfully added user
```

Related Commands

Command	Description
show snmp users	Displays the configured SNMP users on the server.
set snmp user del	Deletes an SNMP user.

set snmp user del

To delete an SNMP user, enter one of the following commands, depending on whether you are using SNMP version 3 or 2c.

set snmp user del 3 *snmp-username*

set snmp user del 2c *community-string*

Syntax Description

3	Specifies SNMP version 3.
snmp-username	SNMP username.
2c	Specifies SNMP version 2c.
community-string	Community string.

Usage Guidelines

For details, see the "Deleting an SNMP User" section on page 26-5.

Examples

The following example shows how to delete an SNMP user:

```
admin: show snmp users
1)  Username: mrtg                      Version: v3
       Level: AuthNoPriv                   Mode: RW

2) Community: public                    Version: v2c
       Level: n/a                          Mode: R

3)  Username: testuser                  Version: v3
       Level: AuthNoPriv                   Mode: RW

admin: set snmp user del 3 testuser
Successfully deleted user

admin: show snmp users
1)  Username: mrtg                      Version: v3
       Level: AuthNoPriv                   Mode: RW

2) Community: public                    Version: v2c
       Level: n/a                          Mode: R
```

Related Commands

Command	Description
show snmp users	Displays the configured SNMP users on the server.
set snmp user add	Adds an SNMP user.

show cdp

To display CDP information for a server, enter the following command.

show cdp {**config** | **list**}

Syntax Description

config	Displays the current CDP configuration on the server.
list	Displays the interfaces on which you can enable or disable CDP.

Usage Guidelines

Use this command to verify the CDP configuration on a server, or to see on which interfaces you can enable CDP on a particular server.

Examples

In the following example, the command output shows the current CDP configuration on a server. This particular example shows the default configuration for all Cisco TelePresence Exchange System servers.

```
admin: show cdp config
  CDP Configuration: Enabled

    Hello Timer : 60 seconds
    Hold Time   : 180 seconds
    Enabled on  : bond0
```

In the following example, the command output from an administration or call engine server shows that only the Bond 0 interface is available for enabling CDP:

```
admin: show cdp list
  Available Interfaces:
     bond0
```

In the following example, the command output from a database server shows that Bond 0 and Bond 1 interfaces are available for enabling CDP:

```
admin: show cdp list
  Available Interfaces:
     bond0
     bond1
```

Related Commands

Command	Description
set cdp enable	Enables CDP for one or all interfaces on a server.
set cdp disable	Disables CDP for one or all interfaces on a server.
set cdp timer	Specifies how often the server sends CDP updates.
set cdp holdtime	Specifies the length of time that the receiving device should hold a CDP packet from this server before discarding it.

show dbip

To display the database virtual IP (VIP) address that is configured on the administration server or call engine server, enter the following command.

show dbip

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command only on the administration server or call engine server.

You can use this command to verify that the correct database VIP address is configured on the administration server or call engine server.

Examples

The following example shows how to display the database VIP address:

```
admin: show dbip
Database IP: 10.22.130.54
```

Related Commands

Command	Description
set adminserver changedbip	Configures the database VIP address that is configured on the administration server.
set sipserver changedbip	Configures the database VIP address that is configured on the call engine server.

show engineip

To display which IP address the call engine server is using to listen for SIP messages, enter the following command.

show engineip

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command only on the call engine server.

If the command output shows an IP address that differs from the IP address of Ethernet 0 (or Bond 0), contact a customer service representative.

Examples

In the following example, the call engine server is listening for SIP messages on 10.22.130.50, which matches the IP address of Bond 0:

```
admin: show engineip
SIP Engine IP: 10.22.130.50

admin: show network eth0
eth0 has been overridden by Network Fault Tolerance.
To view the Ethernet port configuration, please use following command:
show network failover

admin: show network failover
Bond 0
DHCP         : disabled           Status     : up
IP Address   : 10.22.130.50       IP Mask    : 255.255.255.224
Link Detected: no                 Mode       : Auto disabled, N/A, N/A

Ethernet 0
DHCP         : disabled           Status     : up
IP Address   :                    IP Mask    :
Link Detected: yes                Mode       : Auto enabled, Full, 1000MB/s

Ethernet 1
DHCP         : disabled           Status     : up
IP Address   :                    IP Mask    :
Link Detected: yes                Mode       : Auto enabled, Full, 1000MB/s

DNS
Primary      :                    Secondary  :
Options      : timeout:5 attempts:2
Domain       :
Gateway      : 10.22.130.33 on Ethernet bond0
```

Related Commands

Command	Description
set network ip eth0	Changes the IP address of a server.
show network eth0	Displays the Ethernet port configuration.
show network failover	Displays which interfaces are bonded together for network fault tolerance.

show network eth0

To display the details for the Ethernet port on the switch that connects to the network, enter the following command.

show network eth0

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to check the general status of the network connection.

Examples

In the following example, NIC teaming is not enabled on the server:

```
admin# show network eth0
    Ethernet 0
       DHCP         : disabled           Status     : up
       IP Address   : 10.22.139.232      IP Mask    : 255.255.255.224
       Link Detected: yes                Mode       : Auto enabled, Full, 1000 Mbits/s
       Duplicate IP : no

       DNS
       Not configured.
       Gateway      : 10.22.139.225 on Ethernet 0
```

In the following example, NIC teaming is enabled on the server, so the IP address of the server is associated with the Bond 0 interface instead of Ethernet 0:

```
admin: show network eth0
eth0 has been overridden by Network Fault Tolerance.
To view the Ethernet port configuration, please use following command:
show network failover

admin: show network failover
Bond 0
DHCP         : disabled           Status     : up
IP Address   : 10.22.130.58       IP Mask    : 255.255.255.224
Link Detected: no                 Mode       : Auto disabled, N/A, N/A

Ethernet 0
DHCP         : disabled           Status     : up
IP Address   :                    IP Mask    :
Link Detected: yes                Mode       : Auto enabled, Full, 1000MB/s

Ethernet 1
DHCP         : disabled           Status     : up
IP Address   :                    IP Mask    :
Link Detected: yes                Mode       : Auto enabled, Full, 1000MB/s

DNS
Primary      :                    Secondary  :
Options      : timeout:5 attempts:2
Domain       :
Gateway      : 10.22.130.33 on Ethernet bond0
```

Related Commands

Command	Description
set network failover ena	Enables the bond between Ethernet 0 and Ethernet 1 on the administration server or call engine server.
show network failover	Displays which interfaces are bonded together on the server.

show network failover

To display which interfaces are bonded together for network fault tolerance, enter the following command.

show network failover

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

When NIC teaming is enabled on the server (as it is by default), the Cisco TelePresence Exchange System software bonds certain interfaces together for redundancy, depending on the type of server:

Server	Bonded Interfaces
Database server	Bond 0—Ethernet 0 with Ethernet 2 Bond 1—Ethernet 1 with Ethernet 3
Administration server	Bond 0—Ethernet 0 with Ethernet 1
Call engine server	Bond 0—Ethernet 0 with Ethernet 1

Examples

The following example shows that Ethernet 0 and Ethernet 1 are bonded together as Bond 0:

```
admin: show network failover
Bond 0
DHCP         : disabled           Status     : up
IP Address   : 10.22.139.105      IP Mask    : 255.255.255.240
Link Detected: no                 Mode       : Auto disabled, N/A, N/A

Ethernet 0
DHCP         : disabled           Status     : up
IP Address   :                    IP Mask    :
Link Detected: yes                Mode       : Auto enabled, Full, 1000MB/s

Ethernet 1
DHCP         : disabled           Status     : up
IP Address   :                    IP Mask    :
Link Detected: no                 Mode       : Auto enabled, Unknown! (255), 1000MB/s

DNS
Primary      :                    Secondary  :
Options      : timeout:5 attempts:2
Domain       : localdomain
Gateway      : 10.22.139.97 on Ethernet bond0
```

The following example shows that bonding has been disabled on the server:

```
admin: show network failover
Network Fault Tolerance is not configured.
```

Related Commands

Command	Description
set network failover dis	Disables the bond between Ethernet 0 and Ethernet 1 on the administration server or call engine server.
set network failover ena	Enables the bond between Ethernet 0 and Ethernet 1 on the administration server or call engine server.

show role

To display the role of a Cisco TelePresence Exchange System server, enter the following command.

show role

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

None.

Examples

The following example shows sample output from a database server:

```
admin:show role


Host Name    : ctx-db-1
Role         : Database

Date         : Thu Feb 10, 2011 04:51:03
Time Zone    : Coordinated Universal Time (Etc/UTC)
Locale       : en_US.UTF-8

Memory Total:        8290136K
        Free:        7898884K
        Used:         391252K
      Cached:         156724K
      Shared:              0K
     Buffers:          32556K

                       Total            Free            Used
Disk/active          8064272K        6327356K        1654988K (21%)
Disk/inactive        8064304K        7603816K          50832K
```

The following example shows sample output from a call engine server:

```
admin: show role


Host Name    : ctx-engine-a
Role         : Engine
Database Name: ctx-db
Database IP  : 10.22.130.54
Admin Name   :
Admin IP     :

Date         : Fri Sep 10, 2010 16:46:07
Time Zone    : Coordinated Universal Time (Etc/UTC)
Locale       : en_US.UTF-8

Memory Total:        8290136K
        Free:        4613228K
        Used:        3676908K
      Cached:        2744600K
      Shared:              0K
     Buffers:         114360K
```

```
                       Total            Free            Used
Disk/active          8064272K        5359072K        2623272K (33%)
Disk/inactive        8064304K        7603816K          50832K
```

The following example shows sample output from an administration server:

```
admin: show role


Host Name    : ctx-admin-a
Role         : Admin
Database Name: ctx-db
Database IP  : 10.22.130.54
Engine Name  :
Engine IP    :

Date         : Fri Sep 10, 2010 16:51:29
Time Zone    : Coordinated Universal Time (Etc/UTC)
Locale       : en_US.UTF-8

Memory Total:        8290136K
        Free:        6025892K
        Used:        2264244K
      Cached:        1660596K
      Shared:              0K
     Buffers:          80884K

                       Total            Free            Used
Disk/active          8064272K        5891600K        2090744K (27%)
Disk/inactive        8064304K        7603816K          50832K
```

Related Commands

None.

show siplb

To display the SIP load balancer virtual IP (VIP) address and port configuration on the call engine server, enter the following command.

show siplb

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command only on the call engine servers.

Examples

The following example shows the configured SIP load balancer VIP address and port:

```
admin: show siplb
SIP Loadbalancer Host: 10.22.139.103
SIP Loadbalancer Port: 5060
```

The following example shows that the SIP load balancer is not configured on the call engine server:

```
admin: show siplb
SIP Loadbalancer is not enabled/configured on this server.
```

Related Commands

Command	Description
set sipserver siplb ena	Configures the SIP load balancer VIP address and port on the call engine server.
set sipserver siplb dis	Removes the SIP load balancer VIP address and port configuration on the call engine server.

show snmp trapdests

To display the SNMP trap destinations that are configured on a Cisco TelePresence Exchange System server, enter the following command.

show snmp trapdests

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

For details, see the "Configuring SNMP" chapter.

Examples

The following example shows the configured SNMP trap destinations on a server:

```
admin: show snmp trapdests
  1) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = TimTrap                PW   = authpriv
           Level = authnopriv             Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  2) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = trapusr                PW   = trappass
           Level = authnopriv             Hash = md5
        EngineID = 0x8000DEECAFE8111BEEFADE
```

Related Commands

Command	Description
set snmp trapdest add	Adds an SNMP trap destination.
set snmp trapdest del	Deletes an SNMP trap destination.

show snmp users

To display the all SNMP users that are configured on a Cisco TelePresence Exchange System server, enter the following command.

show snmp users

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

For details, see the "Configuring SNMP" chapter.

Examples

The following example shows the configured SNMP users:

```
admin: show snmp users
1)  Username: admin                     Version: v3
       Level: AuthNoPriv                   Mode: RW

2)  Username: tim                       Version: v3
       Level: AuthNoPriv                   Mode: RW

3) Community: TimRO                     Version: v2c
       Level: n/a                          Mode: R

4) Community: TimRW                     Version: v2c
       Level: n/a                          Mode: RW
```

Related Commands

Command	Description
set snmp user add	Adds an SNMP user.
set snmp user del	Deletes an SNMP user.

show trapvip

To see whether the system is configured to include a virtual IP (VIP) address in product-specific SNMP notifications, enter the following command.

show trapvip

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command only on the administration server.

For details, see the following sections:

- Adding a Cluster-Identifying VIP Address to SNMP Notifications, page 26-8
- Removing the Cluster-Identifying VIP Address from SNMP Notifications, page 26-10

Examples

The following example shows that a VIP address is configured to be included in product-specific notifications:

```
admin: show trapvip
SNMP Trap VIP: 10.22.129.200
```

The following example shows that a VIP address is *not* configured to be included in product-specific notifications:

```
admin: show trapvip
SNMP Trap VIP is not enabled/configured on this server.
```

Related Commands

Command	Description
set adminserver trapvip	Adds or removes a virtual IP (VIP) address in product-specific SNMP notifications.

utils network ping

To verify connectivity to a database server, administration server, or call engine server, enter the following command from a network console:

utils network ping *ip-address*

Syntax Description

ip-address	IP address or virtual IP (VIP) address to which you are testing connectivity.

Usage Guidelines

Use this command to verify network connectivity from any Cisco TelePresence Exchange System server to another machine.

Examples

The following example shows how to verify network connectivity from any Cisco TelePresence Exchange System server to another machine:

```
admin: utils network ping 10.22.139.230

PING 10.22.139.230 (10.22.139.230) 56(84) bytes of data.
64 bytes from 10.22.139.230: icmp_seq=0 ttl=62 time=0.285 ms
64 bytes from 10.22.139.230: icmp_seq=1 ttl=62 time=0.189 ms
64 bytes from 10.22.139.230: icmp_seq=2 ttl=62 time=0.193 ms
64 bytes from 10.22.139.230: icmp_seq=3 ttl=62 time=0.187 ms

--- 10.22.139.230 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.187/0.213/0.285/0.043 ms, pipe 2
```

Related Commands

None.

utils patch download

To download the patch to the local patch repository of the server, enter the following command.

utils patch download

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Before you install the patch, you must download it to your designated server.

When you use this command, you are prompted to enter the IP address, username, password, directory, and name of the file to download from the SSH file transfer protocol (SFTP) server. An error occurs if your user credentials are not valid or an invalid field is entered.

Note The location of the patch is not displayed.

Examples

The following example shows how to download the patch from the SFTP server:

```
admin: utils patch download
SFTP server IP: 55.81.143.210
SFTP server port [22]:
User ID: root
Password: ********
Directory containing file to download: /patches/ctx
Name of file to download: BusinessTP-patchbundle-release version number.tar.gz

Download starting.  Depending on your network speed, the download may take several
minutes.

Download completed.
```

Related Commands

Command	Description
utils patch history	Lists the sequence of the patches that have been installed and uninstalled.
utils patch install	Installs the patch on the administration server or call engine server.
utils patch show-patches	Displays the names of the patch files that are downloaded in to the repository.
utils patch uninstall	Uninstalls the patch that has already been installed on either the administration server or call engine server.

utils patch history

To list the sequence of the patches that have been installed and uninstalled, enter the following command.

utils patch history

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

A new entry is added to the patch history each time a patch is installed or uninstalled. Each entry displays the date, time of action of when the install or uninstall occurred, whether the entry is for an install or uninstall, and the version of the patch that is installed or uninstalled.

A message is displayed if no patches were installed.

Examples

The following example shows the history of each patch:

```
admin: utils patch history

Patch History:

Wed Jan 18 21:20:20 PST 2012 install release version number.P2
Wed Jan 18 21:21:48 PST 2012 uninstall release version number.P2
```

Related Commands

Command	Description
utils patch download	Downloads the patch to the local patch repository of the server.
utils patch install	Installs the patch on the administration server or call engine server.
utils patch show-patches	Displays the names of the patch files that are downloaded in to the repository.
utils patch uninstall	Uninstalls the patch that has already been installed on either the administration server or call engine server.

utils patch install

To install the patch on the administration server or call engine server, enter the following command.

utils patch install *patch-file*

Syntax Description

patch-file	Name of the patch file you want to install.

Usage Guidelines

Use this command to install the patch file that you previously downloaded on the administration server or call engine server. To locate the names of the previously downloaded patch files, use the utils patch show-patches command. You must gracefully halt the operation of the administration and call engine servers before continuing (see the utils service adminserver stop command or utils service sipserver stop command). When the patch is installed on all the servers, you must start the services again.

A message is displayed if the patch installation is successful or not. You will also be prompted for the following conditions:

- The name of the patch file is not entered correctly.
- The patch is not found in the repository.
- The patch is already installed.
- The install.sh script fails or is not found.

Examples

The following example shows how to install the patch on the administration server:

```
admin: utils service adminserver stop
adminserver...................Stopped
admin: utils patch install BusinessTP-patchbundle-release version number.tar.gz

Please make sure that the admin and sip services are stopped on all computers
before continuing with this install.

Do you want to continue with this install (yes/no)? yes

Opening BusinessTP-patchbundle-release version number.tar.gz...

./artifacts/
./artifacts/ctc_userInterface.xml
./install.sh
./properties.sh
./README.txt
./uninstall.sh
./VERSION
==================== CTC patch install ====================
Current version is release version number
Role of this node is Admin
Current version (short) 1.1.0
Patch version: release version number

Installing patch on admin server.
Saved ctc_userInterface.xml /common/patches/release version number/original/
cp artifacts/ctc_userInterface.xml to /usr/local/platform/conf/cli/interface/
Finished patching....
```

```
Installation Complete

When all computers have been patched, restart the services.

admin: utils service adminserver start
adminserver.................Started - PID <27494>
```

Related Commands

Command	Description
utils patch download	Downloads the patch to the local patch repository of the server.
utils patch history	Lists the sequence of the patches that have been installed and uninstalled.
utils patch show-patches	Displays the names of the patch files that are downloaded in to the repository.
utils patch uninstall	Uninstalls the patch that has already been installed on either the administration server or call engine server.
utils service adminserver start	Starts an administration server after your server is down or after you use the **utils service adminserver stop** command.
utils service adminserver stop	Gracefully stops an administration server.
utils service sipserver start	Starts a call engine server that is down.
utils service sipserver stop	Gracefully stops a call engine server.

utils patch show-patches

To display the names of the patch files that are downloaded in to the repository, enter the following command.

utils patch show-patches

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to display the patch files that are in the repository. A message is displayed if no patch files were found in the repository.

Examples

The following example shows how to display the patch files:

```
admin: utils patch show-patches

Patch Files:

BusinessTP-patchbundle-release version number.tar.gz
```

Related Commands

Command	Description
utils patch download	Downloads the patch to the local patch repository of the server.
utils patch history	Lists the sequence of the patches that have been installed and uninstalled.
utils patch install	Installs the patch on the administration server or call engine server.
utils patch uninstall	Uninstalls the patch that has already been installed on either the administration server or call engine server.

utils patch uninstall

To uninstall the patch that has already been installed on either the administration server or call engine server, enter the following command.

utils patch uninstall

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to uninstall the patch that you recently installed. Before you uninstall the patch, you must gracefully halt the operation of the administration server and call engine server (see the utils service adminserver stop command or utils service sipserver stop command). When the patch is uninstalled on all the servers, you must start the services again.

A message is displayed if the patch uninstall is successful or not. Only the most recently applied patch is uninstalled. You cannot uninstall multiple patches to revert the system back to the original state. If you attempt to uninstall more than one patch, a message is displayed that another install must be performed before any additional uninstalls can be performed.

Examples

The following example shows how to uninstall the patch on the administration server:

```
admin: utils service adminserver stop
adminserver.....................Stopped
admin: utils patch uninstall

Do you want to continue with this uninstall (yes/no)? yes

==================== CTC patch uninstall ====================
Role of this node is Admin

Patch version: release version number

Uninstalling patch on admin server.
Restoring original files /common/patches/release version
number/original//ctc_userInterface.xml to /usr/local/platform/conf/cli/interface/


Uninstall Complete

When all computers have been unpatched, restart the services.

admin: utils service adminserver start
adminserver.................Started - PID <7120>
```

Related Commands

Command	Description
utils patch download	Downloads the patch to the local patch repository of the server.
utils patch history	Lists the sequence of the patches that have been installed and uninstalled.
utils patch install	Installs the patch on the administration server or call engine server.

Command	Description
utils patch show-patches	Displays the names of the patch files that are downloaded in to the repository.
utils service adminserver start	Starts an administration server after your server is down or after you use the **utils service adminserver stop** command.
utils service adminserver stop	Gracefully stops an administration server.
utils service sipserver start	Starts a call engine server that is down.
utils service sipserver stop	Gracefully stops a call engine server.

utils service adminserver start

To start an administration server after your server is down or after you use the **utils service adminserver stop** command, enter the following command.

utils service adminserver start

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to gracefully start an administration server.

Examples

In the following example, the **utils service adminserver start** command was entered because the server status indicated that the administration server was not running:

```
admin: utils service adminserver status
adminserver.................Not running
admin: utils service adminserver start
adminserver.................Started - PID <23338>
admin: utils service adminserver status
adminserver.................Starting - PID <23338>
admin: utils service adminserver status
adminserver.................Running - PID <23338>
```

Related Commands

Command	Description
utils service adminserver stop	Gracefully stops an administration server.
utils service adminserver status	Displays the status of the administration server.

utils service adminserver status

To check the status of an administration server, enter the following command.

utils service adminserver status

Syntax Description

This command has no arguments or keywords.

Examples

The following example shows that the administration server is up and running:

admin: **utils service adminserver status**

```
adminserver.............................Not running
```

The following example shows that the administration server was stopped:

admin: **utils service adminserver status**

```
adminserver.............................<Pid: 3223> Not Running
```

Related Commands

Command	Description
utils service database status	Checks the status of the database server.
utils service sipserver status	Checks the status of the call engine server.

utils service adminserver stop

To gracefully stop an administration server, enter following command.

utils service adminserver stop

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command whenever you need to gracefully halt operation of an administration server.

If you enter this command, the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB will stop responding. After you start the administration server by entering the utils service adminserver start command, the product-specific MIB will start responding.

Examples

The following example shows how to gracefully halt the operation of the administration server:

```
admin: utils service adminserver status
adminserver.................Running - PID <10817>
admin: utils service adminserver stop
adminserver..............Stopped
admin: utils service adminserver status
adminserver.................Not running
```

Related Commands

Command	Description
utils service adminserver start	Gracefully starts the administration server.
utils service adminserver status	Displays the status of the administration server.

utils service corosync status

To check the status of a corosync service on the current server, enter the following command.

utils service corosync status

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command on the administration, call engine, and database servers.

The corosync utility determines which database server takes on the primary role in the cluster. Corosync uses input from each server in the cluster to make this determination and runs on each server as a service.

Examples

The following example shows that the corosync service is up and running on all the Cisco TelePresence Exchange System servers:

```
admin: utils service corosync status
corosync.................Running - PID <18613>
```

The following example shows that the corosync service is not running on all the Cisco TelePresence Exchange System servers:

```
admin: utils service corosync status
corosync.................Not running
```

Related Commands

Command	Description
utils service crm status	Monitors the Cluster Resource Manager (CRM) status on all the Cisco TelePresence Exchange System servers.

utils service crm status

To monitor the Cluster Resource Manager (CRM) status on all the Cisco TelePresence Exchange System servers, enter the following command.

utils service crm status

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to check and monitor the CRM status.

In the example, the header shows a summary of the following status fields:

- Date, time of action, and version of when the cluster status last provided a successful output.
- The machine, which is used as the current domain controller (DC), indicates which of the six servers is the current domain controller. During normal operation, all six servers show the same DC and it should be the partition with the quorum. For example, if one server shows a different DC or the partition does not have a quorum, check the network connectivity between the servers. A minimum of four servers must always be online to satisfy the quorum requirement.
- The expected number of servers that are known to the cluster is six.
- The expected number of known resources that are configured is three.

Examples

The following example shows a summary of the current CRM status on the servers, displays the status of all six servers as online, displays the status of one database server with three resources as started, and displays the expected behavior for the four entries on the administration and call engine servers:

```
admin: utils service crm status
============
Last updated: Tue Apr  3 21:20:53 2012
Stack: openais
Current DC: feature8-db2 - partition with quorum
Version: 1.0.9-89bd754939df5150de7cd76835f98fe90851b677
6 Nodes configured, 6 expected votes
3 Resources configured.
============

Online: [ feature8-engine2 feature8-admin2 feature8-db2 feature8-engine1 feature
8-admin1 feature8-db1 ]

 Resource Group: mysql
     mysql_filesystem   (ocf::heartbeat:Filesystem):    Started feature8-db2
     mysql_vip  (ocf::heartbeat:IPaddr2):       Started feature8-db2
     mysql_server       (ocf::heartbeat:mysql): Started feature8-db2
 Master/Slave Set: mysql_replication
     Masters: [ feature8-db2 ]
     Slaves: [ feature8-db1 ]
 Clone Set: gateway_conn_monitor
     Started: [ feature8-engine2 feature8-db2 feature8-admin2 feature8-engine1 f
eature8-admin1 feature8-db1 ]

Failed actions:
   drbd_mysql:0_monitor_0 (node=feature8-admin2, call=5, rc=5, status=complete)
: not installed
```

```
   drbd_mysql:0_monitor_0 (node=feature8-engine2, call=5, rc=5, status=complete
): not installed
   drbd_mysql:0_monitor_0 (node=feature8-engine1, call=5, rc=5, status=complete
): not installed
   drbd_mysql:0_monitor_0 (node=feature8-admin1, call=5, rc=5, status=complete)
: not installed
```

Related Commands

Command	Description
utils service corosync status	Checks the status of a corosync service on the current server.

utils service database drbd disable-ha

To disable high availability (HA) and set the current secondary database server to take over the primary HA role, enter the following command.

utils service database drbd disable-ha

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to set the current secondary database server to act as the primary server. This situation allows the primary database server to assume the primary HA role even when it did not meet the minimum quorum of four votes. For details, see the "Recovering from a Situation Where Three or More Servers Failed" section on page 33-1.

Examples

The following example shows how to disable HA on a database server:

```
admin: utils service database drbd disable-ha
Disabling quorum requirement... [Done]
```

Related Commands

Command	Description
utils service database drbd enable-ha	Enables HA on the database server.
utils service database status	Checks the status of the database server.

utils service database drbd discard-node

To reset a database server to function in the secondary high-availability (HA) role, enter the following command.

utils service database drbd discard-node

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to recover from split brain mode. For details, see the "Split Brain Recovery" chapter.

Note When you enter this command, all data on that database server is deleted and cannot be recovered. Make sure that you carefully follow the instructions for split brain recovery.

Examples

The following example shows how to reset a database server to function as the secondary database server:

```
admin: utils service database drbd discard-node
This command will make this node as Secondary
Trying to assume secondary role......... [Done]
Ensuring DRBD volume unmounted...
Ensuring DRBD role is Secondary...
Discarding local MySQL data..... [Done]
```

Related Commands

Command	Description
utils service database drbd keep-node	Resets a database server to function in the primary high-availability (HA) role.
utils service database status	Checks the status of the database server.

utils service database drbd enable-ha

To enable high availability (HA) after manually recovering from a failed primary database server, enter the following command.

utils service database drbd enable-ha

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command only if you had disabled HA by using the utils service database drbd disable-ha command. For details, see the "Recovering from a Situation Where Three or More Servers Failed" section on page 33-1.

Caution Entering this command will temporarily interrupt MySQL service. Cisco recommends that you use this command only during maintenance windows. During the MySQL service interruption, new calls will not be able to connect to meetings, and users will not be able to schedule meetings.

Examples

The following example shows how to enable HA on a database server:

```
admin: utils service database drbd enable-ha
Enabling quorum requirement... [Done]
```

Related Commands

Command	Description
utils service database drbd disable-ha	Disables HA on the database server.
utils service database status	Checks the status of the database server.

utils service database drbd force-discard-node

To reset the metadata for the Distributed Replicated Block Device (DRBD) and set a database server to function in the secondary high-availability (HA) role, enter the following command.

utils service database drbd force-discard-node

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to recover when the DRBD metadata is corrupted. For details, see the "Recovering from Corrupted DRBD Metadata" section on page 30-6. The DRBD feature synchronizes the secondary database with changes that are made on the primary database.

Note When you enter this command, all data on that database server is deleted and cannot be recovered. Make sure that you carefully follow the instructions for corrupted DRBD metadata recovery.

Examples

The following example shows how to reset the DRBD metadata and set a database server to function as the secondary database server:

```
admin: utils service database drbd force-discard-node
Shutting down Heartbeat...
Stopping High-Availability services:
[  OK  ]
Ensuring DRBD volume unmounted...
umount: /dev/drbd0: not mounted
Taking down DRBD Resource...
Recreating DRBD meta-data...
NOT initialized bitmap
Bringing up DRBD...
Starting Heartbeat...
Starting High-Availability services:
[  OK  ]
 [Done]
```

Related Commands

Command	Description
utils service database drbd force-keep-node	Resets the DRBD metadata and sets a database server to function in the primary high-availability (HA) role.
utils service database status	Checks the status of the database server.

utils service database drbd force-keep-node

To reset the metadata for the Distributed Replicated Block Device (DRBD) and set a database server to function in the primary high-availability (HA) role, enter the following command.

utils service database drbd force-keep-node

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to recover when the DRBD metadata is corrupted. For details, see the "Recovering from Corrupted DRBD Metadata" section on page 30-6. The DRBD feature synchronizes the secondary database with changes that are made on the primary database.

Examples

The following example shows how to reset the DRBD metadata and set a database server to function as the primary database server:

```
admin: utils service database drbd force-keep-node
This command will make this node as Primary
Trying to assume primary role......... [Done]
Overwriting peer data... [Done]
```

Related Commands

Command	Description
utils service database drbd force-discard-node	Resets the DRBD metadata and sets a database server to function in the secondary high-availability (HA) role.
utils service database status	Checks the status of the database server.

utils service database drbd force-mysql-reset

To reformat the Distributed Replicated Block Device (DRBD) partition, restore a backup MySQL installation, and set a database server to function in the primary high-availability (HA) role, enter the following command.

utils service database drbd force-mysql-reset

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to recover when the MySQL database is corrupted. For details, see the "Corrupted MySQL Database Recovery" chapter.

Caution All data in the MySQL database will be lost and unrecoverable after entering this command. Make sure that you follow the corrupted MySQL database recovery procedures carefully.

Examples

The following example shows how to reset the DRBD metadata and set a database server to function as the primary database server:

```
admin: utils service database drbd force-mysql-reset
This command will make this node as Primary
This command will make this node as Primary
Trying to assume primary role......... [Done]
Temporarily stopping mon services...
Stopping mon daemon: [FAILED]
Stopping MySQL...
 ERROR! MySQL manager or server PID file could not be found!
Ensuring DRBD volume unmounted...
Rebuilding DRBD filesystem...
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
5898240 inodes, 11796480 blocks
589824 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=12582912
360 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424

Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 21 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
Remounting DRBD volume...
Retrieving backup MySQL files...
Starting MySQL...
```

```
Starting MySQL. ERROR! Manager of pid-file quit without updating file.
Starting mon...
Starting mon daemon: [  OK  ]
 [Done]
```

The server then restarts, is assigned the primary HA role, and initiates the synchronization process.

Related Commands

Command	Description
utils service database status	Checks the status of the database server.

utils service database drbd keep-node

To reset a database server to function in the primary high-availability (HA) role, enter the following command.

utils service database drbd keep-node

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to recover from split brain mode or after replacing a failed initial primary database server. For details, see one of the following sections:

- Split Brain Recovery, page 30-1
- Recovering from a Situation Where Three or More Servers Failed, page 33-1

Examples

The following example shows how to reset a database server to function as the current primary database server:

```
admin: utils service database drbd keep-node
This command will make this node as Primary
Trying to assume primary role......... [Done]
Reconnecting to MySQL......... [Done]
```

Related Commands

Command	Description
utils service database drbd discard-node	Resets a database server to function in the secondary high-availability (HA) role.
utils service database status	Checks the status of the database server.

utils service database status

To check the status of a database server, enter the following command.

utils service database status

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to check the status, configuration, and high-availability (HA) role of a database server, for example, during the installation and synchronization process.

The command output displays both the initial configured HA role and the current HA role of the node. The initial configured HA role is determined by whether you specified the primary role during installation. After the database servers are synchronized and actively in use, you typically only need to see the current HA role in the command output.

The following sample status values indicate an active and healthy system:

- Corosync is running.
- MySQL is running (current primary database server only).
- The Connection Sync Status field is “Connected.”

  A Connection Sync Status value of “WFConnection” means that the server is waiting for a connection from its redundant peer, for example, after the installation but before database synchronization.
- The role values indicate that one server has the primary role, and the other server has the secondary role, specifically:
  - The role state on the left shows the HA role of the server on which you are viewing the command output.
  - The role state on the right shows the HA role of the redundant peer.
- The Disk Status field is “UpToDate” for both servers, specifically:
  - The disk status on the left shows the disk status of the server on which you are viewing the command output.
  - The disk status on the right shows the disk status of the redundant peer.

During the initial synchronization, the command output indicates the progress of the synchronization process.

This command is also used to diagnose and recover from various database problems. See the following sections:

- Split Brain Recovery, page 30-1
- Corrupted MySQL Database Recovery, page 31-1
- Server Failure Recovery, page 33-1

Examples

Sample output from the current primary database server:

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : primary
The current HA role of this node                 : primary
The database vip address                         : 10.22.130.61
Node name                                        : ctx-db-1
Node IP address                                  : 10.22.130.50
Corosync status                                  : Running PID <19250>
Current Designated Controller (DC)               : ctx-db-1 - partition with quorum
MySQL status                                     : Running pid  15633
Connection Sync Status                           : Connected
Role (this-node/peer-node)                       : Primary/Secondary
Disk Status (this-node/peer-node)                : UpToDate/UpToDate
--------------------------------------------------------------------------------
```

Sample output from the current secondary database server:

```
admin: utils service database status
--------------------------------------------------------------------------------
The initial configured HA role of this node      : secondary
The current HA role of this node                 : secondary
The database vip address                         : 10.22.130.61
Node name                                        : ctx-db-2
Node IP address                                  : 10.22.130.58
Corosync status                                  : Running PID <26656>
Current Designated Controller (DC)               : ctx-db-1 - partition with quorum
MySQL status                                     : Not running (only runs on
database server with current role primary.)
Connection Sync Status                           : Connected
Role (this-node/peer-node)                       : Secondary/Primary
Disk Status (this-node/peer-node)                : UpToDate/UpToDate
--------------------------------------------------------------------------------
```

Related Commands

Command	Description
utils service sipserver status	Checks the status of a call engine server.
utils service adminserver status	Checks the status of the administration server.

utils service nodemanager start

To start a Cisco Tomcat service that is down, enter the following command.

utils service nodemanager start

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to gracefully start a Cisco Tomcat service on the administration, call engine, and database servers.

Examples

In the following example, the **utils service nodemanager start** command was entered because the service status indicated that the Cisco Tomcat service was not running.

```
admin: utils service nodemanager status
tomcat.........................Not running
admin: utils service nodemanager start
tomcat.........................Starting - PID <22970>
admin: utils service nodemanager status
tomcat.........................Running - PID <22970>
```

Related Commands

Command	Description
utils service nodemanager status	Checks the status of a Cisco Tomcat service after installation or during general operations.
utils service nodemanager stop	Gracefully stops a Cisco Tomcat service.

utils service nodemanager status

To check the status of a Cisco Tomcat service after installation or during general operations, enter the following command:

utils service nodemanager status

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to check the status of the Cisco Tomcat service on the administration, call engine, and database servers.

Examples

The following example shows that the Cisco Tomcat service is up and running:

```
admin: utils service nodemanager status
tomcat.........................Running - PID <15959>
```

The following example shows that the Cisco Tomcat service stopped:

```
admin: utils service nodemanager status
tomcat.........................Not running
```

Related Commands

Command	Description
utils service nodemanager start	Starts a Cisco Tomcat service that is down.
utils service nodemanager stop	Gracefully stops a Cisco Tomcat service.

utils service nodemanager stop

To gracefully stop a Cisco Tomcat service, enter the following command.

utils service nodemanager stop

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command whenever you need to gracefully halt operation of a Cisco Tomcat service on the administration, call engine, and database servers.

Examples

The following example shows how to gracefully halt the operation of the Cisco Tomcat service:

```
admin: utils service nodemanager status
tomcat.........................Running - PID <22970>
admin: utils service nodemanager stop
tomcat......................Stopped
admin: utils service nodemanager status
tomcat.........................Not running
```

Related Commands

Command	Description
utils service nodemanager start	Starts a Cisco Tomcat service that is down.
utils service nodemanager status	Checks the status of a Cisco Tomcat service after installation or during general operations.

utils service sipserver start

To gracefully start a call engine server that is down, enter the following command.

utils service sipserver start

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to gracefully start a call engine server.

Examples

In the following example, the **utils service sipserver start** command was entered because the server status indicated that the call engine server was not running:

```
admin: utils service sipserver status
sipserver.............................Not running
admin: utils service sipserver start
sipserver.............................Starting - PID <14891>
admin: utils service sipserver status
sipserver.............................Running - PID <14891>
```

Related Commands

Command	Description
utils service sipserver stop	Gracefully stops the call engine server.
utils service sipserver status	Displays the status of the call engine server.

utils service sipserver status

To check the status of a call engine server after installation or during general operations, enter the following command.

utils service sipserver status

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

None.

Examples

The following example shows that the call engine server is up and running:

```
admin: utils service sipserver status
sipserver.............................<Pid: 3223> running
```

The following example shows that the call engine server stopped:

```
admin: utils service sipserver status
sipserver.............................Not running
```

Related Commands

Command	Description
utils service adminserver status	Checks the status of the administration server.
utils service database status	Checks the status of the database server.

utils service sipserver stop

To gracefully stop a call engine server, enter the following command.

utils service sipserver stop *service*

Syntax Description

This command has no arguments or keywords.

Examples

The following example shows how to gracefully halt the operation of the call engine server:

```
admin: utils service sipserver status
sipserver.............................Running - PID <13097>
admin: utils service sipserver stop
sipserver.................................Stopped
admin: utils service sipserver status
sipserver.............................Not running
```

Related Commands

Command	Description
utils service sipserver start	Gracefully starts a call engine server.
utils service sipserver status	Checks the status of a call engine server.

utils snmp get

To get the SNMP data for a discrete MIB object, enter one of the following commands, depending on whether you are using SNMP version 3 or 2c.

utils snmp get 3 *username ip-address object-id* [*file*]

utils snmp get 2c *community-string ip-address object-id* [*file*]

Syntax Description

3	Specifies SNMP version 3.
username	SNMP username.
2c	Specifies SNMP version 2c.
community-string	Community string.
ip-address	IP address of the server that you want to query. To query the server on which you are logged in to the CLI, enter the localhost IP address 127.0.0.1.
object-id	Object ID (OID).
file	(Optional) Filename or directory path to the file for the output.

Usage Guidelines

This command enables you to query a server for the value of a discrete MIB object, or one piece of management data. If you instead want the values of a table MIB object, which contains multiple pieces of management data, use the **utils snmp walk** command.

This command is typically used to troubleshoot SNMP issues. See the "Troubleshooting SNMP" section on page 26-12.

Examples

The following example shows how to get the system description (sysDescr.0) from SNMP:

```
admin: utils snmp get 2c private 10.22.140.73 1.3.6.1.2.1.1.1.0
This command may temporarily impact CPU performance.
Continue (y/n)? y
iso.3.6.1.2.1.1.1.0 STRING: "\"Hardware:7845I3, 2  Intel(R) Xeon(R) CPU           E5540  @
2.53GHz, 8192 MB Memory: Software:UCOS 4.0.0.0-31 Product:Cisco TelePresence Exchange
System:1.0.1.0.1103-6\""
```

Related Commands

Command	Description
show snmp users	Displays the configured SNMP users on the server.
utils snmp walk	Get the SNMP data for a table MIB object.

utils snmp hardware-agents restart

To restart the hardware agent for an IBM server, enter the following command.

utils snmp hardware-agents restart

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to restart the hardware agent for an IBM server without rebooting the server.

Typically, this command is used only if the hardware agent on the server fails, that is, when IBM MIBs do not respond while the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB and other MIBs continue to work.

Examples

The following example shows how to restart the hardware agent for an IBM server:

```
admin: utils snmp hardware-agents restart
Stopping SNMP agents ...
SNMP agents stopped
Starting SNMP agents ...
SNMP agents started
```

Related Commands

None.

utils snmp walk

To get the SNMP data for a table MIB object, enter one of the following commands, depending on whether you are using SNMP version 3 or 2c.

utils snmp walk 3 *username ip-address object-id*

utils snmp walk 2c *community-string ip-address object-id*

Syntax Description

3	Specifies SNMP version 3.
username	SNMP username.
2c	Specifies SNMP version 2c.
community-string	Community string.
ip-address	IP address of the server that you want to query. To query the server on which you are logged in to the CLI, enter the localhost IP address 127.0.0.1.
object-id	Object ID (OID).
file	*Not supported.*

Usage Guidelines

This command enables you to query a server for the values of a table MIB object, which contains multiple pieces of management data. If you instead want to query a server for the value of a discrete MIB object, or one piece of management data, use the **utils snmp get** command.

This command is typically used to troubleshoot SNMP issues. See the "Troubleshooting SNMP" section on page 26-12.

Examples

The following example shows how to query an administration server for the values of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB objects:

```
admin: utils snmp walk 2c public 127.0.0.1 1.3.6.1.4.1.9.9.758
This command may temporarily impact CPU performance.
Continue (y/n)? y
iso.3.6.1.4.1.9.9.758.1.1.1.1.2.1 Hex-STRING: 8A 96 01 49 2B 3B 42 0D 01 2B 3B 45 0C 70 00
0D
iso.3.6.1.4.1.9.9.758.1.1.1.1.3.1 STRING: "cisco"
iso.3.6.1.4.1.9.9.758.1.1.1.1.4.1 STRING: "description 1"
iso.3.6.1.4.1.9.9.758.1.1.1.1.5.1 STRING: "null"
iso.3.6.1.4.1.9.9.758.1.1.2.1.2.1 Hex-STRING: 8A 96 01 49 2B 3B 42 0D 01 2B 3B 60 A4 E7 00
1D
iso.3.6.1.4.1.9.9.758.1.1.2.1.2.2 Hex-STRING: 8A 96 01 49 2B 3B 42 0D 01 2B 3B 60 A5 1C 00
28
iso.3.6.1.4.1.9.9.758.1.1.2.1.3.1 STRING: "San Francisco"
iso.3.6.1.4.1.9.9.758.1.1.2.1.3.2 STRING: "San FranciscoLMLM"
iso.3.6.1.4.1.9.9.758.1.1.2.1.4.1 STRING: "null"
iso.3.6.1.4.1.9.9.758.1.1.2.1.4.2 STRING: "8a9601492b3b420d012b3b60a4e7001d"
iso.3.6.1.4.1.9.9.758.1.1.2.1.5.1 Hex-STRING: 8A 96 01 49 2B 3B 42 0D 01 2B 3B 45 0C 70 00
0D
iso.3.6.1.4.1.9.9.758.1.1.2.1.5.2 Hex-STRING: 8A 96 01 49 2B 3B 42 0D 01 2B 3B 45 0C 70 00
0D
iso.3.6.1.4.1.9.9.758.1.1.3.1.2.1 Hex-STRING: 8A 96 01 49 2B A4 08 1A 01 2B AC 20 FD 10 03
E8
```

```
iso.3.6.1.4.1.9.9.758.1.1.3.1.3.1 STRING: "testSNMP"
iso.3.6.1.4.1.9.9.758.1.1.3.1.4.1 STRING: "null"
iso.3.6.1.4.1.9.9.758.1.1.3.1.5.1 Gauge32: 48
iso.3.6.1.4.1.9.9.758.1.1.3.1.6.1 INTEGER: 2
iso.3.6.1.4.1.9.9.758.1.1.3.1.7.1 Hex-STRING: 8A 96 01 49 2B 3B 42 0D 01 2B 3B 45 0C 70 00
0D
iso.3.6.1.4.1.9.9.758.1.1.4.1.1.2.1 Hex-STRING: 8A 96 01 49 2B BC 9D 2A 01 2B C0 38 4C AC
01 C9
iso.3.6.1.4.1.9.9.758.1.1.4.1.1.2.2 Hex-STRING: 8A 96 01 49 2B 64 00 20 01 2B 6A 26 BD FD
03 27
iso.3.6.1.4.1.9.9.758.1.1.4.1.1.2.3 Hex-STRING: 8A 96 01 49 2B 54 91 68 01 2B 54 96 59 3A
00 2A
iso.3.6.1.4.1.9.9.758.1.1.4.1.1.2.4 Hex-STRING: 8A 96 01 49 2B 3B 42 0D 01 2B 3B D3 2D F6
01 04
iso.3.6.1.4.1.9.9.758.1.1.4.1.1.3.1 STRING: "agile5-ctsman2"
iso.3.6.1.4.1.9.9.758.1.1.4.1.1.3.2 STRING: "tps1"
iso.3.6.1.4.1.9.9.758.1.1.4.1.1.3.3 STRING: "agile5-ctms"
iso.3.6.1.4.1.9.9.758.1.1.4.1.1.3.4 STRING: "agile4-ivr-resource"
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

Related Commands

Command	Description
show snmp users	Displays the configured SNMP users on the server.
utils snmp get	Gets the SNMP data for a discrete MIB object.

utils system restart

To restart a database, administration, or call engine server, enter the following command:

utils system restart

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

If you restart the server over SSH, you will lose your connection while the server restarts.

Examples

The following example shows how to restart a database server:

```
admin: utils system restart

Do you really want to restart ?

Enter (yes/no)? yes
Current DRBD state is Connected. OK to proceed with restart.


 Appliance is being Restarted ...
Shutting down Service Manager will take some time..
\   Service Manager shutting down services... Please Wait
DONE!!!!

Broadcast message from root (Thu Feb 10 04:55:47 2011):

The system is going down for reboot NOW!
Waiting .

Operation succeeded

restart now.
```

Related Commands

Command	Description
utils system shutdown	Shuts down a Cisco TelePresence Exchange System server.

utils system shutdown

To shut down a database, administration, or call engine server, enter the following command.

utils system shutdown

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to shut down the system for maintenance, for example, to upgrade software.

Examples

The following example shows how to shut down a database server:

```
admin: utils system shutdown

Do you really want to shutdown ?

Enter (yes/no)? yes
Current DRBD state is Connected. OK to proceed with restart.


 Appliance is being Powered - Off ...
Shutting down Service Manager will take some time..
\   Service Manager shutting down services... Please Wait
DONE!!!!

Broadcast message from root (Thu Mar 24 19:47:04 2011):

The system is going down for system halt NOW!
Waiting .

Operation succeeded

shutdown now.
```

Related Commands

Command	Description
utils system restart	Restarts a Cisco TelePresence Exchange System server.

APPENDIX D

MIB Reference

This appendix provides reference information for the one product-specific MIB that is currently available for the Cisco TelePresence Exchange System: CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB.

CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB

This MIB provides product-specific configuration, status, statistics, events, errors, and alarm notifications for the following devices:

- All nodes in the Cisco TelePresence Exchange System server cluster.
- Cisco TelePresence Exchange System–configured resources which provide the signaling, media services, scheduling, and other functions that enable the system to deliver an end-to-end solution.

This MIB is implemented only on the administration server, which provides management interfaces for all nodes in the server cluster and for the configured resources.

The CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB uses the OID 1.3.6.1.4.1.9.9.758.

For details and to download the MIB, go to: ftp://ftp.cisco.com/pub/mibs/v2/CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB.my.

For reference information about the MIB, see the following sections:

Also see the "Configuration Tasks for the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB" section on page D-10.

Update Intervals for SNMP Tables

Table D-1 shows how long it may take for information, such as a configuration change or event, to take effect in the relevant SNMP table. For example, after adding a new resource, it could take up to 30 seconds before the resource entry shows up in the ctxResourceTable.

Table D-1 SNMP Table Update Intervals for CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB

Type	Update Interval	Tables
Configuration-based tables	30 seconds	ctxServiceProviderTable ctxRegionTable ctxOrganizationTable ctxResourceTable ctxSipConfigTable ctxMediaCapacityConfigTable ctxMeetingConfigTable ctxClusterNodeTable
Statistic tables	5 seconds	ctxResourceStatsTable ctxAllocStatsTable
Peak history tables	15 seconds	ctxPeakHistAllocTable ctxPeakHistAllocPoolTable
Event history table	5 seconds	ctxErrorHistoryTable

Overall Health System Status Objects

Table D-2 defines the states and conditions of objects in the overall system status subtree ctxSystemStatusObjects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB.

Table D-2 Overall Health System Status Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB

Object	Status	Description
ctxAdminServersStatus	NORMAL	Both administration servers are fully operational and able to process requests.
	WARNING	One of the administration servers is down, but the other is still functional.
	ERROR	Both administration servers are offline or not functional. This status would never be returned because SNMP would not work if both administration servers were offline.
ctxCallEnginesStatus	NORMAL	Both call engine servers are fully operational and able to process requests.
	WARNING	One of the call engine servers is down, but the other is still functional.
	ERROR	Both call engine servers are offline or not functional.

Table D-2 Overall Health System Status Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB (continued)

Object	Status	Description
ctxDatabaseServersStatus	NORMAL	Both database servers are fully operational and able to process requests. In this mode, the current primary database server is active, the current secondary database server is available in the standby state, and the database is replicating.
	WARNING	One of the database servers is down, or the database is not replicating. In this mode, there is no standby database server.
	ERROR	Both database servers are offline or not functional. Having no functional database server is a problem for the entire Cisco TelePresence Exchange System server cluster.
ctxResourceStatus	NORMAL	According to the resource monitoring probes, all configured and enabled resources are operational. See the "Resource Monitoring" section on page 26-3.
	WARNING	One resource is offline or not functional.
	ERROR	Two or more resources are offline or not functional.
ctxSystemConfigStatus	NORMAL	The system configuration is complete enough to enable the scheduling, attending, and One-Button-to-Push (OBTP) functions of the system.
	WARNING	*Not supported.*
	ERROR	The system configuration is not complete and is blocking one of the key functions of the system.
ctxSystemBackupStatus	NORMAL	Backup is scheduled, and the last backup was successful.
	WARNING	Backup is not scheduled or not properly configured.
	ERROR	Last backup has failed.

Table Objects

Table D-3 Table Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB

Table Object	OID	Description
ctxServiceProviderTable	1.3.6.1.4.1.9.9.758.1.1.1	This table specifies the configuration information for service providers as they are configured in the Cisco TelePresence Exchange System. Service provider entries provide a logical grouping of regions, organizations, and resources.
ctxRegionTable	1.3.6.1.4.1.9.9.758.1.1.2	This table specifies the configuration information for regions as they are configured in the Cisco TelePresence Exchange System. A region is defined as a set of resources that are similar in terms of network latency, jitter, and quality of service. Typically, a region is a geographic area such as the Americas, Europe, or Asia Pacific, but a region can be a smaller set of resources (for example, U.S. East and U.S. West regions).

Table D-3 Table Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB (continued)

Table Object	OID	Description
ctxOrganizationTable	1.3.6.1.4.1.9.9.758.1.1.3	This table specifies the configuration information for an organization as configured in the Cisco TelePresence Exchange System. Organization entries provide a logical grouping of customer endpoints and resources.
ctxResourceTable	1.3.6.1.4.1.9.9.758.1.1.4.1	This table specifies the configuration information for resources as they are configured in the Cisco TelePresence Exchange System. A resource is a server or network device that is configured in the Cisco TelePresence Exchange System to provide call signaling, media services, scheduling, or solution functions. A resource may have additional configuration items, such as the ctxSipConfigTable object. Each of the other ctxResourceObjects tables are indexed by this resource entry. If a resource has SIP configurations, there will be a entry in the ctxSipConfigEntry indexed by this ctxResourceIndex.
ctxSipConfigTable	1.3.6.1.4.1.9.9.758.1.1.4.2	This table specifies the SIP configuration attributes for a resource. Only resources that have SIP attributes will have an entry in this table.
ctxMediaCapacityConfigTable	1.3.6.1.4.1.9.9.758.1.1.4.3	This table specifies the media capacity configuration attributes for a resource. Only resources that have media capacity attributes will have an entry in this table.
ctxMeetingConfigTable	1.3.6.1.4.1.9.9.758.1.1.4.4	This table specifies the meeting configuration attributes for a resource. Only resources that have meeting attributes will have an entry in this table.
ctxClusterNodeTable	1.3.6.1.4.1.9.9.758.1.1.5	This table specifies the configuration information for cluster nodes as they are configured in the Cisco TelePresence Exchange System. A cluster node is a server within the Cisco TelePresence Exchange System, such as an administration server, call engine server, or database server.
ctxResourceStatsTable	1.3.6.1.4.1.9.9.758.1.3.1	This table specifies the run-time resource statistics.
ctxAllocStatsTable	1.3.6.1.4.1.9.9.758.1.3.2	This table specifies the run-time scheduling port allocation statistics.
ctxRegionStatsTable	1.3.6.1.4.1.9.9.758.1.3.3	This table specifies the run-time statistics for regions for scheduling port allocations and call setup failures. This table is similar to the ctxAllocStatsTable table, except that this table provides statistics per region for all resources.
ctxPeakHistAllocTable	1.3.6.1.4.1.9.9.758.1.3.4.3	This table specifies the run-time peak statistics for resource port allocations. This table contains peak port allocations per resource for ctxHistMaxIntervals. The management entity can use this table to monitor the peak port allocations per interval. Setting ctxPeakHistMaxIntervals to 0 would disable this table and clear all entries in the table.

Table D-3 Table Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB (continued)

Table Object	OID	Description
ctxPeakHistAllocPoolTable	1.3.6.1.4.1.9.9.758.1.3.4.4	This table specifies the run-time peak port allocation statistics for all resources within a region. This table contains peak port allocations per region for ctxHistMaxIntervals. The management entity can use this table to monitor the peak port allocations per interval. Setting ctxPeakHistMaxIntervals to 0 would disable this table and clear all entries in the table.
ctxErrorHistoryTable	1.3.6.1.4.1.9.9.758.1.4.4	This table contains a history of alarms and events that are generated by the Cisco TelePresence Exchange System. This table is a real-time history table of alarms and events for the Cisco TelePresence Exchange System. When the table reaches its capacity, which is specified in ctxErrorHistoryTableSize, the agent will purge the oldest entry. The management entity can receive real-time events when an object is inserted into this table by configuring ctxErrorHistoryEventNotifyEnable to TRUE and receiving ctxErrorHistoryEvent notifications.

Trap Notification Objects

Table D-4 Trap Notification Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB

Notification Object	OID	Description
ciscoCTXSysAdminServersStatusChg	1.3.6.1.4.1.9.9.758.0.1	This notification is sent when the ctxAdminServersStatus changes. ctxStatusChangeNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysDatabaseServersStatusChg	1.3.6.1.4.1.9.9.758.0.2	This notification is sent when the ctxDatabaseServerStatus changes. ctxStatusChangeNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysCallEnginesStatusChg	1.3.6.1.4.1.9.9.758.0.3	This notification is sent when the ctxCallEnginesStatus changes. ctxStatusChangeNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysResourceStatusChg	1.3.6.1.4.1.9.9.758.0.4	This notification is sent when the ctxResourceStatus changes. ctxStatusChangeNotifyEnable controls whether or not this notification is sent.

Table D-4 Trap Notification Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB (continued)

Notification Object	OID	Description
ciscoCTXSysSystemConfigStatusChg	1.3.6.1.4.1.9.9.758.0.5	This notification is sent when the ctxSystemConfigStatus changes. ctxStatusChangeNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysSystemBackupStatusChg	1.3.6.1.4.1.9.9.758.0.6	Backup status is a warning if no backup has been scheduled correctly. Status is an error if the last backup has failed. This notification is sent when the ctxSystemBackupStatus changes. ctxStatusChangeNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysLicenseFailure	1.3.6.1.4.1.9.9.758.0.7	License errors are a stateless event. License errors are generated once a day for system-wide license errors or when there is a call that violates a license. The lack of license errors after 24 hours could be considered cleared. This notification is sent for demo license errors: • Warnings begin 5 days prior to demo license expiration if you have not installed a permanent license. • Error messages begin immediately after the demo license expiration if the user has not installed a permanent license. ctxLicenseAlarmNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysUserAuthFailure	1.3.6.1.4.1.9.9.758.0.8	User authentication failures are generated after three consecutive login failures by the same user to either the administration console or CLI of the Cisco TelePresence Exchange System. ctxAuthFailureNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysClusterNodeDown	1.3.6.1.4.1.9.9.758.0.9	This notification is sent when there is a network connectivity or probe monitor failure to a cluster node from the administration server. ctxClusterNodeAlarmNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysClusterNodeUp	1.3.6.1.4.1.9.9.758.0.10	This notification is sent when the cluster node connectivity is restored or when the probe monitor is successful in monitoring the node after it had been down. ctxClusterNodeAlarmNotifyEnable controls whether or not this notification is sent.

Table D-4 Trap Notification Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB (continued)

Notification Object	OID	Description
ciscoCTXSysResourceDown	1.3.6.1.4.1.9.9.758.0.11	This notification is sent when there is a network connectivity or probe monitor failure to the resource. This can be a SIP OPTION PING, XML-RPC, or network connectivity failure. The ctxNotifyMessage contains the failure details. ctxResourceAlarmNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysResourceUp	1.3.6.1.4.1.9.9.758.0.12	This notification is sent when the resource connectivity is restored or when the probe monitor is successful in monitoring the resource after it had been down. ctxResourceAlarmNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysResourceAllocFailure	1.3.6.1.4.1.9.9.758.0.13	This notification is sent when a resource allocation failure occurs. ctxResourceAlarmNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysCallSetupFailure	1.3.6.1.4.1.9.9.758.0.14	This notification is sent when there is a call-setup or routing failure between the Cisco TelePresence Exchange System and a resource. The cause for the setup failure is detailed in ctxNotifyMessage. ctxCallFailureNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysCallAbnormalDisconnect	1.3.6.1.4.1.9.9.758.0.15	This notification is sent when there is an abnormal call disconnect. The call disconnect reason is detailed in ctxNotifyMessage. ctxCallFailureNotifyEnable controls whether or not this notification is sent.
ciscoCTXSysErrorHistoryEvent	1.3.6.1.4.1.9.9.758.0.16	This notification is sent when a new ctxErrorHistoryEntry is created. If the event being logged does not have an organization name, then this varbind entry is an empty string value. ctxErrorHistoryEventNotifyEnable controls whether or not this notification is sent.

Read-Write Objects

Table D-5 Read-Write Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB

Object	OID	Description
ctxStatusChangeNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.1	This object specifies whether the status change traps should be enabled or disabled. Setting this to true enables the notifications. Setting this to false disables the notifications. Default is true (enabled). This object controls the generation of the following notifications: • ciscoCTXSysAdminServersStatusChg • ciscoCTXSysDatabaseServersStatusChg • ciscoCTXSysCallEnginesStatusChg • ciscoCTXSysResourceStatusChg • ciscoCTXSysSystemConfigStatusChg • ciscoCTXSysSystemBackupStatusChg
ctxLicenseAlarmNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.2	This object specifies whether the license alarm traps should be enabled or disabled. Setting this to true enables the notifications. Setting this to FALSE disables the notifications. Default is true (enabled). This object controls the generation of the notification ciscoCTXSysLicenseFailure.
ctxAuthFailureNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.3	This object specifies whether the authentication failure traps should be enabled or disabled. Setting this to true enables the notifications. Setting this to false disables the notifications. The default setting for authentication failures is false (disabled) in order to prevent unnecessary event flooding. This object controls the generation of the notification ciscoCTXSysUserAuthFailure.
ctxClusterNodeAlarmNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.4	This object specifies whether the cluster node alarm traps should be enabled or disabled. Setting this to true enables the notifications. Setting this to false disables the notifications. Default is true (enabled). This object controls the generation of the following notifications: • ciscoCTXSysClusterNodeDown • ciscoCTXSysClusterNodeUp

Table D-5 Read-Write Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB (continued)

Object	OID	Description
ctxResourceAlarmNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.5	This object specifies whether the resource alarm traps should be enabled or disabled. Setting this to true enables the notifications. Setting this to false disables the notifications. Default is true (enabled). This object controls the generation of the following notifications: • ciscoCTXSysResourceDown • ciscoCTXSysResourceUp • ciscoCTXSysResourceAllocFailure
ctxCallFailureNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.6	This object specifies whether the call failure traps should be enabled or disabled. Setting this to true enables the notifications. Setting this to false disables the notifications. Default is true (enabled). This object controls the generation of the following notifications: • ciscoCTXSysCallSetupFailure • ciscoCTXSysCallAbnormalDisconnect
ctxErrorHistoryEventNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.7	This object specifies whether the error event history traps should be enabled or disabled. Setting this to true enables the notifications. Setting this to false disables the notifications. Notifications and other errors are logged in the error history table. Enabling this object may cause duplication of events that are already duplicates of other notifications. This may be the desired behavior of the management system. Use ctxErrorHistoryMaxSeverity to specify the maximum severity level to be logged and sent via a notification. Default is false (disabled). This object controls the generation of the notification ciscoCTXSysErrorHistoryEvent.
ctxErrorHistoryTableSize	1.3.6.1.4.1.9.9.758.1.4.1	This object specifies the maximum number of entries that the ctxErrorHistoryTable can contain. When the capacity of the ctxErrorHistoryTable is reached, the oldest entry in the table is deleted to accommodate a new entry. A value of ‘0’ disables the history table. The default value is set to 100 entries.

Table D-5 Read-Write Objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB (continued)

Object	OID	Description
ctxErrorHistoryMaxSeverity	1.3.6.1.4.1.9.9.758.1.4.2	Defines the maximum severity of the event messages that the history table will contain. The default is notice(5), which can be changed by setting the object. Available options: • emergency(0) • alert(1) • critical(2) • error(3) • warning(4) • notice(5) • info(6) • debug(7)
ctxPeakHistMaxIntervals	1.3.6.1.4.1.9.9.758.1.3.4.1	This object specifies the number of time intervals that are kept in the history tables ctxPeakHistAllocTable and ctxPeakHistAllocPoolTable. The default is 96 intervals, which at the ctxPeakHistIntTime default of 15 minutes, stores peak values for 24 hours. A value of 0 will disable peak history tables from collecting data. The range is from 5 to 1440 intervals. Changing this value will reset and clear both ctxPeakHistAllocTable and ctxPeakHistAllocPoolTable table entries.
ctxPeakHistIntTime	1.3.6.1.4.1.9.9.758.1.3.4.2	This object specifies the time interval in minutes. The default is 15 minutes. The range is from 1 to 1440 minutes. Changing this value will reset and clear both ctxPeakHistAllocTable and ctxPeakHistAllocPoolTable table entries.

Configuration Tasks for the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB

Configuration tasks are described in the following topics:

- Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, page 26-10
- Adding a Cluster-Identifying VIP Address to SNMP Notifications, page 26-8

- Removing the Cluster-Identifying VIP Address from SNMP Notifications, page 26-10

APPENDIX E

Data Migration

Revised July 3, 2012

This appendix describes how the Cisco TelePresence Exchange System migrates data from Release 1.0.(x) to Release 1.1, and how the administration console graphical user interface has changed between the two releases.

The following sections are included:

About the Migration Behavior for Media Bridge Resources and Resource Groups

When migrating media bridge resources (Cisco TelePresence Multipoint Switch [CTMS], Cisco TelePresence MCU MSE 8510 [MSE 8510], and Cisco TelePresence Server MSE 8710 [TPS]) from Release 1.0(x) to Release 1.1, the system automatically creates region-specific resource groups in the following manner:

- All media bridge resources that are reserved for large meetings are contained within one resource group per region.
- All media bridge resources that are not reserved for large meetings are contained within one resource group per region.
- Up to two resource groups per region are created, where one of the resource groups contains only media bridge resources that are reserved for large meetings and the other resource group contains only media bridge resources that are not reserved for large meetings.
- Names are assigned to the new resource groups based on the name of the associated region and whether or not the resource group contains resources that are reserved for large meetings. For example, if the resource group contains resources that are placed in the San Jose region and reserved for large meetings, then the system will name the resource group San Jose Large Resource Group.

  Table E-1 provides examples of the system behavior for migrating media bridge resources to new resource groups.

Table E-1 Migration Behavior Examples for Media Bridge Resources and Resource Groups

Before Data Migration	After Data Migration
CTMS resource that was not reserved for large meetings was placed in the San Jose region.	CTMS resource that was not reserved for large meetings is placed in a resource group named San Jose Resource Group.
TPS resource that was reserved for large meetings was placed in the San Jose region.	TPS resource that was reserved for large meetings is placed in a resource group named San Jose Large Resource Group.
MSE 8510 resource that was reserved for large meetings was placed in the San Francisco region.	MSE 8510 resource that was reserved for large meetings is placed in a resource group named San Francisco Large Resource Group.

- By default, the system configures new resource groups with a guaranteed reservation type with the following dedication percentage and booking percentage settings:
  - For a resource group that contains resources that are reserved for large meetings, both the dedication percentage and booking percentage are set to 100%.
  - For a resource group that contains resources that are not reserved for large meetings, the dedication percentage is set to 80%, and the booking percentage is set to 100%.

About the Migration Behavior for Meet-Me and Rendezvous Meetings

Caution If you scheduled both Meet-Me and Rendezvous meetings, all the Rendezvous meetings will be deleted. Before you start the upgrade process, verify that all the Rendezvous meetings have been manually saved so that they can be created again.

When meetings are migrated during the upgrade to Release 1.1, the Host PINs and Automatic Meeting Extension meeting fields will be disabled.

For detailed information about the requirements and prerequisites to upgrade the software on the Cisco TelePresence Exchange System, see the "Upgrading the Software" chapter.

Administration Console Comparisons

The following sections describe the administration console user interface comparisons between Release 1.0.(x) to Release 1.1:

Media Bridge Resources Comparisons

The following sections describe the field comparisons for the media bridge resources:

CTMS Resources Field Comparisons

Table E-2 describes the Cisco TelePresence Multipoint Switch (CTMS) resources field comparisons.

Table E-2 CTMS Resources Field Comparisons

Release 1.0.(x) Field	Release 1.0.(x) Field Removed	Release 1.0.(x) Scenario	Replaced With...	Release 1.1 Scenario
Test CTMS	Yes	The Test check box allowed the CTMS to be available for test meetings only. A test system was not available for scheduling regular meetings.	—	The test resource concept is not supported.
Region	Yes	The resources were contained in the regions.	The Resource Group field.	The reservation type is configured by indicating a specific resource. The resources are contained in the resource groups. The resource groups are contained in the regions.

TPS Resources Field Comparisons

Table E-3 describes the Cisco TelePresence Server MSE 8710 (TPS) resources field comparisons.

Table E-3 TPS Resources Field Comparisons

Release 1.0.(x) Field	Release 1.0.(x) Field Removed	Release 1.0.(x) Scenario	Replaced With...	Release 1.1 Scenario
Test TPS	Yes	The Test check box allowed you to reserve the TPS for test meetings only. When serving as a test system, the resource was not available as a resource for scheduling regular meetings.	—	The test resource concept is not supported.
Region	Yes	The resources were contained in the regions.	The Resource Group field.	The reservation type is configured by indicating a specific resource. The resources are contained in the resource groups. The resource groups are contained in the regions.

MSE 8510 Resources Field Comparisons

Table E-4 describes the Cisco TelePresence MCU MSE 8510 (MSE 8510) resources field comparisons.

Table E-4 MSE 8510 Resources Field Comparisons

Release 1.0.(x) Field	Release 1.0.(x) Field Removed	Release 1.0.(x) Scenario	Replaced With...	Release 1.1 Scenario
Test MSE 8510	Yes	The Test check box allowed you to reserve the MSE 8510 for test meetings only. The system was not available as a resource for scheduling regular meetings.	—	The test resource concept is not supported.
Region	Yes	The resources were contained in the regions.	The Resource Group field.	The resources are contained in the resource groups. The resource groups are contained in the regions.

Customers Comparisons

Table E-5 describes the region field comparisons.

Table E-5 Region Field Comparisons

Release 1.0.(x) Field	Release 1.0.(x) Field Removed	Release 1.0.(x) Scenario	Replaced With...	Release 1.1 Scenario
Service Provider	Yes	The region was associated with any service provider.	—	The region is not associated with any service provider.

Table E-6 describes the organizations field comparisons.

Table E-6 Organizations Field Comparisons

Release 1.0.(x) Field	Release 1.0.(x) Field Removed	Release 1.0.(x) Scenario	Replaced With...	Release 1.1 Scenario
Direct Dial Enabled	Yes	This check box enabled direct-dial for an organization.	The Enforce Whitelisting field.	Restrictions are enforced on direct-dial calls between this organization and other organizations under the same service provider (also known as intra-SP direct calls).

Endpoint Management Comparisons

Table E-7 describes the media profiles field comparisons.

Table E-7 Media Profiles Field Comparisons

Release 1.0.(x) Field	Release 1.0.(x) Field Removed	Release 1.0.(x) Scenario	Replaced With...	Release 1.1 Scenario
Video Bandwidth	Yes	This optional field allowed you to specify the maximum video bandwidth for the endpoint type.	—	—
Audio Bandwidth	Yes	This optional field allowed you to set the maximum audio bandwidth available for the endpoint type.	—	—
Participant Type	Yes	This drop-down list allowed you to choose the value that corresponded to this endpoint type.	The Protocols check boxes.	You can choose one or more media protocols that are supported by this endpoint type.

Collaboration Services Comparisons

Table E-8 describes the meetings field comparisons under collaboration services.

Table E-8 Meetings Field Comparisons

Release 1.0.(x) Field	Release 1.0.(x) Field Removed	Release 1.0.(x) Scenario	Replaced With...	Release 1.1 Scenario
Is Remote Meeting	Yes	The Is Remote Meeting field indicated a remote meeting. A yes or no value was displayed depending on the choice.	The Meeting Type field.	The Meeting Type field displays all four meeting types.
Test	Yes	The Test check box allowed the system to run test meetings. This check box was displayed only when scheduling a Meet-Me meeting.	—	The test resource concept is not supported.
Request Specific Resource	Yes	The Request Specific Resource check box allowed the system to display a drop-down list of available resources.	—	—
Additional Bridge Capabilities	Yes	The Additional Bridge Capabilities field allowed you to set the required bridge capabilities for unprovisioned endpoints in the meeting.	The Additional Media Profiles field.	All existing meetings, which specified additional bridge capabilities, are converted to the applicable additional media profiles. This scenario occurs when you are modifying a future meeting that was originally scheduled before the data migration.

APPENDIX F

IP Communications Required by the Cisco TelePresence Exchange System

Added July 19, 2012

This appendix contains the following sections:

Firewall and Access List Considerations

The Cisco TelePresence Exchange System is a component of the Cisco Unified Communications suite and is designed to be deployed on a converged IP network. You can use access control lists (ACLs) and firewalls to secure IP communications between the servers in the Cisco TelePresence Exchange System and other solution components.

This appendix covers the specific TCP and UDP ports that you must allow between each server component (administration, call engine and database) in the Cisco TelePresence Exchange System system and other solution components. Other solution components and resources used by the Cisco TelePresence Exchange System have their own set of security requirements and needs for IP communications with other devices. These additional requirements are not within the scope of this appendix, but must be considered if a firewall or ACL is used to further secure those devices.

When you install the Cisco TelePresence Exchange System, you place the administration, call engine, and database servers in a dedicated VLAN. Do not place any firewall (transparent and/or routed) between the administration, call engine, and database servers. Doing so causes issues with multicast communications. The Cisco TelePresence Exchange System servers implement an application firewall that restricts communication to the server. The application firewall rules can be viewed by logging in to the CLI of the server and entering the **utils firewall ipv4 list** command.

This appendix does not provide guidance on specific router, firewall, or IPS platforms or configurations you should use to secure IP communications between Cisco TelePresence Exchange System and other devices. We strongly recommend that you thoroughly test your Cisco TelePresence Exchange System components with your specific security configuration prior to deploying the configuration in a production deployment.

Note Firewalls that rely on Application Layer Inspection in order to dynamically open or close certain UDP ports may not support the specific SIP protocol implementation used by Cisco TelePresence, or may not be able to inspect the contents of the application layer protocol because it is encrypted.

Ports that are Used Between Cisco TelePresence Exchange System Servers

Table F-1 lists the ports used between Cisco TelePresence Exchange System servers.

Caution Do not place any firewall (transparent and/or routed) between the administration, call engine, and database servers. The Cisco TelePresence Exchange System servers share a dedicated VLAN and implement an application firewall that restricts communications.

Table F-1 Ports Required for Cisco TelePresence Exchange System Administration Server IP Communications

Protocol	Type (TCP or UDP)	Source Device:Port	Destination Device:Port	Comments
ActiveMQ	TCP	Administration:61616	Administration, Call Engine, or Database:Ephemeral	Used by all Cisco TelePresence Exchange System servers to send events via the Active MQ Event Framework.
	TCP	Administration, Call Engine, or Database:Ephemeral	Administration:61616	Used by all Cisco TelePresence Exchange System servers to send events via the Active MQ Event Framework.
Zookeeper	TCP	Administration, Call Engine, or Database:Ephemeral	Administration, Call Engine, or Database:2888, 3888	Used by Zookeeper.
Tomcat	TCP	Administration, Call Engine, or Database:Ephemeral	Administration, Call Engine, or Database:9010	Used by the NodeManager WS API.
Corosync	UDP	Administration, Call Engine, or Database:Ephemeral	Administration, Call Engine, or Database:9999, 10000	Used by Corosync.

Administration Server Ports

Table F-2 lists the ports required by the administration server.

Table F-2 Ports Required for Cisco TelePresence Exchange System Administration Server IP Communications

Protocol	Type (TCP or UDP)	Source Device:Port	Destination Device:Port	Comments
CDP	N/A	Administration, Call Engine, or Database:N/A	Cisco Catalyst Switch:N/A	Used to advertise the existence of a server to the upstream Cisco Catalyst Ethernet Switch to which the server is attached and learn which Virtual LAN (VLAN) it should use to tag packets. CDP is a layer 2 protocol and does not use TCP or UDP for transport.
ICMP	N/A	Any:N/A	Any:N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, by using an ICMP echo request/response). A device may occasionally send an ICMP unreachable to indicate that a device or port is no longer reachable. A device may send ICP time-exceeded to indicate that the Time to Live (TTL) of a packet is exceeded.
NTP	UDP	Administration, Call Engine, or Database:123	NTP server:123	Used to synchronize the hardware clock on the Cisco TelePresence Exchange System server with an NTP server.
DNS	UDP	Administration: Ephemeral	DNS server:53	Used to resolve host names to IP addresses. **Note** DNS is not supported on the Cisco TelePresence Exchange System servers in release 1.1. We recommend that you keep DNS disabled on the administration, call engine, and database servers.
Flow-Thru	TCP	Administration: Ephemeral	Cisco TelePresence Manager:8080, 8443	Used between the Cisco TelePresence Exchange System and the Cisco TelePresence Manager for One-Button-to-Push (OBTP) scheduling via XML/SOAP API.
		Administration: Ephemeral	Cisco TelePresence Server MSE 8710:80	XML_RPC: Used to configure the Cisco TelePresence Server MSE 8710.
		Administration: Ephemeral	Cisco TelePresence MCU MSE 8510:80	XML_RPC: Used to configure the Cisco TelePresence MCU MSE 8510.
		Administration: Ephemeral	Cisco Unified Communications Manager:8443	Used by the Cisco TelePresence Exchange System to request SFTP/SCP transfer of CDR records for intra-company (direct dial) hosted calls.
		Cisco Unified Communications Manager: Ephemeral	Administration:22	Used by the Cisco Unified Communications Manager to send CDR records to the administration server via SFTP/SCP.

Table F-2 Ports Required for Cisco TelePresence Exchange System Administration Server IP Communications

Protocol	Type (TCP or UDP)	Source Device:Port	Destination Device:Port	Comments
HTTP—Admin UI	TCP	Any client:Ephemeral	Administration:80, 8080	Used to access the administration console web interface.
Event API	TCP	Administration: Ephemeral	Any:80 (default—can use any port)	Used by the Cisco TelePresence Exchange System to send HTTP SOAP/XML POST events to configured event notification management systems.
SSH	TCP	Any client:Ephemeral	Administration:22	Used to access the administrative CLI interface of the Cisco TelePresence Exchange System.
SNMP	UDP	Any client:Ephemeral	Administration:161	Used for get/set SNMP queries from a management station to the Cisco TelePresence Exchange System server.
	UDP	Administration, Call Engine, or Database:Ephemeral	SNMP Management Station:162	Used to send SNMP traps to a management station.
JBoss	TCP	Any:Ephemeral	Administration, Call Engine:1100	Used on administration and call engine servers by the JBoss High Availability—Java Naming and Directory Interface (HA-JNDI) service.
	TCP	Any:Ephemeral	Administration, Call Engine, or Database:32768-61000	Ephemeral port range.
	UDP	Any:Ephemeral	Administration, Call Engine, or Database:32768-61000	Ephemeral port range.
Tomcat	TCP	Any client:Ephemeral	Administration, Call Engine, or Database:9010	Used by the Upgrade application (on the administration server) and by the NodeManager WS API (on the administration, call engine, and database servers).

Call Engine Server Ports

Table F-3 lists the ports required by the call engine server.

Table F-3 Ports Required for Cisco TelePresence Exchange System Call Engine Server IP Communications

Protocol	Type (TCP or UDP)	Source Device:Port	Destination Device:Port	Comments
CDP	N/A	Administration, Call Engine, or Database:N/A	Cisco Catalyst Switch:N/A	Used to advertise the existence of a server to the upstream Cisco Catalyst Ethernet Switch to which the server is attached and learn which Virtual LAN (VLAN) it should use to tag packets. CDP is a layer 2 protocol and does not use TCP or UDP for transport.
ICMP	N/A	Any:N/A	Any:N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, by using an ICMP echo request/response). A device may occasionally send an ICMP unreachable to indicate that a device or port is no longer reachable. A device may send ICP time-exceeded to indicate that the Time to Live (TTL) of a packet is exceeded.
NTP	UDP	Administration, Call Engine, or Database:123	NTP server:123	Used to synchronize the hardware clock on the Cisco TelePresence Exchange System server with an NTP server.
DNS	UDP	Administration, Call Engine, or Database:Ephemeral	DNS server:53	Used to resolve host names to IP addresses. **Note** DNS is not supported on the Cisco TelePresence Exchange System servers in release 1.1. We recommend that you keep DNS disabled on the administration, call engine, and database servers.
Flow-Thru	TCP	Cisco TelePresence Server MSE 8710: Ephemeral	Call Engine:5050	Used by the Cisco TS MSE 8710 to send events to the call engine servers.
		Cisco TelePresence MCU MSE 8510: Ephemeral	Call Engine:5050	Used by the MCU MSE 8510 to send events to the call engine servers.
VXML	TCP	IVR router:Ephemeral	Call Engine:80, 8080	Used for VXML interaction for IVR prompt downloads.
SSH	TCP	Any client:Ephemeral	Call Engine:22	Used to access the administrative CLI interface of the Cisco TelePresence Exchange System.
SNMP	UDP	Any client:Ephemeral	Call Engine:161	Used for get/set SNMP queries from a management station to the Cisco TelePresence Exchange System server.
	UDP	Administration, Call Engine, or Database:Ephemeral	SNMP Management Station:162	Used to send SNMP traps to a management station.

Table F-3 Ports Required for Cisco TelePresence Exchange System Call Engine Server IP Communications (continued)

Protocol	Type (TCP or UDP)	Source Device:Port	Destination Device:Port	Comments
SIP	TCP	Any:Ephemeral	Call Engine:5060	Used for SIP protocol over TCP.
	UDP	Any:Ephemeral	Call Engine:5060	Used for SIP protocol over UDP.
JBoss	TCP	Administration, Call Engine, or Database:Ephemeral	Call Engine:4446	eCache peer discovery & Socket for JBoss Remote Connector used by Unified Invoker.
	TCP	Administration, Call Engine, or Database:Ephemeral	Call Engine:1098	Socket Naming service used to receive RMI requests from client proxies.
	TCP	Administration, Call Engine, or Database:Ephemeral	Call Engine:1099	JBoss listening socket for the Naming service.
	TCP	Administration or Call Engine:1100	Any:Ephemeral	Used on administration and call engine servers by the JBoss High Availability—Java Naming and Directory Interface (HA-JNDI) service.
	TCP	Administration, Call Engine, or Database:Ephemeral	Call Engine:1101	HA-JNDI Rmi Port.
	UDP	Administration, Call Engine, or Database:Ephemeral	Call Engine:1102	HA-JNDI Auto Discovery Port.
	TCP	Administration, Call Engine, or Database:Ephemeral	Call Engine:3873	JBoss Invoker location.
	TCP	Administration, Call Engine, or Database:Ephemeral	Call Engine:4457	Socket for JBoss Messaging 1.x.
	TCP	Administration, Call Engine, or Database:Ephemeral	Call Engine:4458	Bisocket Transport Connector secondary port.
	TCP	Administration, Call Engine, or Database:Ephemeral	Call Engine:7900	JBoss port used for the JGroups 'jbm-data' stack.
	TCP	Any:Ephemeral	Call Engine:32768-61000	Ephemeral port range.
	UDP	Any:Ephemeral	Call Engine:32767-61000	Ephemeral port range.

Table F-3 Ports Required for Cisco TelePresence Exchange System Call Engine Server IP Communications (continued)

Protocol	Type (TCP or UDP)	Source Device:Port	Destination Device:Port	Comments
IGMP	N/A	Call Engine:N/A	IGMPv2/v3 multicast:N/A	IGMP v2 and v3—used to maintain the multicast memberships.
	N/A	Mrouter (IGMPv2/v3):N/A	Call Engine:N/A	IGMP v2 and v3—used to maintain the multicast memberships.
Tomcat	TCP	Any client:Ephemeral	Administration, Call Engine, or Database:9010	Used by the Upgrade application (on the Administration server) and by the NodeManager WS API (on the Administration, Call Engine, and Database servers).

Database Server Ports

Table F-4 lists the ports required by the database server.

Table F-4 Ports Required for Cisco TelePresence Exchange System Database Server IP Communications

Protocol	Type (TCP or UDP)	Source Device:Port	Destination Device:Port	Comments
CDP	N/A	Administration, Call Engine, or Database:N/A	Cisco Catalyst Switch:N/A	Used to advertise the existence of a server to the upstream Cisco Catalyst Ethernet Switch to which the server is attached and learn which Virtual LAN (VLAN) it should use to tag packets. CDP is a layer 2 protocol and does not use TCP or UDP for transport.
ICMP	N/A	Any:N/A	Any:N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, by using an ICMP echo request/response). A device may occasionally send an ICMP unreachable to indicate that a device or port is no longer reachable. A device may send ICP time-exceeded to indicate that the Time to Live (TTL) of a packet is exceeded.
NTP	UDP	Database:123	NTP server:123	Used to synchronize the hardware clock on the Cisco TelePresence Exchange System server with an NTP server.
DNS	UDP	Database:Ephemeral	DNS server:53	Used to resolve host names to IP addresses. **Note** DNS is not supported on the Cisco TelePresence Exchange System servers in release 1.1. We recommend that you keep DNS disabled on the administration, call engine, and database servers.
SSH	TCP	Any client:Ephemeral	Database:22	Used to access the administrative CLI interface of the Cisco TelePresence Exchange System.

Table F-4 Ports Required for Cisco TelePresence Exchange System Database Server IP Communications (continued)

Protocol	Type (TCP or UDP)	Source Device:Port	Destination Device:Port	Comments
SNMP	UDP	Any client:Ephemeral	Database:161	Used for get/set SNMP queries from a management station to the Cisco TelePresence Exchange System server.
	UDP	Database:Ephemeral	SNMP Management Station:162	Used to send SNMP traps to a management station.
DRBD	TCP	Any:Ephemeral	Database:7788	Used for database replication.
MySQL	TCP	Administration, Call Engine, or Database:Ephemeral	Database:3306	Used for MySQL client access from other Cisco TelePresence Exchange System servers (administration, call engine, and database).
High Availability	UDP	Database:Ephemeral	Database:694	Heartbeat—High Availability Clustering between database servers.
	TCP	Any:Ephemeral	Administration, Call Engine, or Database:32768-61000	Ephemeral port range.
	UDP	Any:Ephemeral	Administration, Call Engine, or Database:32768-61000	Ephemeral port range.
Tomcat	TCP	Any client:Ephemeral	Administration, Call Engine, or Database:9010	Used by the Upgrade application (on the administration server) and by the NodeManager WS API (on the administration, call engine, and database servers).

GLOSSARY

A

ACE — *See* Cisco Application Control Engine (ACE).

access control list (ACL) — Feature that filters incoming or outgoing traffic based on a set of rules that are applied to specified fields in the messages. You can configure an ACL on an incoming or outgoing interface. You can allow or deny traffic based on criteria such as the source and destination IP addresses and port numbers.

active/active — Redundancy configuration in which two units actively participate in the system during normal operation. If one unit fails, the workload of both units is processed by the remaining active unit. A load balancer may be used to facilitate active/active redundancy. *See also* load balancer.

active/standby — Redundancy configuration in which the primary unit actively participates in the system and the secondary unit remains in standby mode. If the primary unit fails, the secondary unit becomes active.

ad hoc meeting — A meeting that begins immediately (in contrast to a scheduled meeting, which starts at a future time).

admin context — On the ACE, you can define a single context or multiple contexts. By default, the ACE creates a single context named the admin context. Multiple contexts use virtualization to partition the ACE into multiple virtual devices. Each context can contain its own set of policies, interfaces, resources, and administrators.

administration console — Provides a graphical user interface for provisioning and monitoring the Cisco TelePresence Exchange System.

administration server — Provides the application programming interface (API) and the administration console for the Cisco TelePresence Exchange System.

administrator — A user role that has access to all setup, configuration, and monitoring functionality in the administration console. This role can add or modify API users (but only the system administrator role can add or modify other administrator users).

application programming interface (API) — Programmatic interface used by a software application program to make requests of another software application.

attending phone number — The phone number that participants dial to connect to a meeting.

C

call detail records (CDRs) Real-time call detail records collected by the Cisco TelePresence Exchange System and forwarded to the service provider for use by a billing support system (BSS).

call engine server Server that manages all call signaling for the Cisco TelePresence Exchange System services. The call engine server supports the active/active mode of redundancy. *See also* active/active.

capacity Refers to the amount of resources reserved or consumed on the multipoint media bridge that is hosting a Meet-Me or Rendezvous meeting. The Cisco TelePresence Exchange System documentation set generally uses the term segment as a measure of the amount of capacity allocated to or used by an endpoint on a media bridge during a meeting time frame. See also segment.

Cisco Aggregation Series Router Provides SIP session border control for the Cisco TelePresence Exchange System. *See also* session border controller (SBC).

Cisco Application Control Engine (ACE) Provides traffic load balancing of HTTP and SIP traffic to the Cisco TelePresence Exchange System server cluster. The ACE is available as a standalone appliance or as a service module for the Catalyst 6500 switch.

Cisco TelePresence Exchange System An integrated video service-creation platform that enables service providers and strategic partners to offer secure cloud-based managed and hosted Cisco TelePresence and business video services.

Cisco TelePresence IP phone Used by meeting participants in the Cisco TelePresence room to initiate meetings. During the meeting, the phone provides access to features such as call muting, call hold, and placing a basic audio call.

Cisco TelePresence ISDN GW MSE 8321 Cisco TelePresence MSE 8000 Series service module that provides inter-working with ISDN endpoints.

Cisco TelePresence Manager Provides scheduling integration for a cluster of Cisco TelePresence Multipoint Switch resources. Cisco TelePresence Manager can provide interoperability with scheduling groupware (such as Microsoft Outlook), and enables One-Button-to-Push (OBTP) functionality for provisioned endpoints. *See also* One-Button-to-Push (OBTP).

Cisco TelePresence MCU MSE 8510 Cisco TelePresence MSE 8000 Series service module that provides inter-working with single-screen H.323 and ISDN standards-based telepresence endpoints.

Cisco TelePresence Multipoint Switch A multipoint control unit that provides media switching and other features for multipoint meetings.

Cisco TelePresence Server MSE 8710 Cisco TelePresence MSE 8000 Series service module that provides inter-working with single-screen and multi-screen telepresence endpoints.

Cisco TelePresence Video Communication Server (Cisco VCS) Extends face-to-face video collaboration across networks and organizations by supporting any-to-any video and telepresence communications. When an enterprise wants to deploy Cisco TelePresence or third-party H.323 and ISDN standards-based endpoints, the enterprise must install at least one Cisco VCS.

Cisco Unified Communications Manager (Unified CM) Provides configuration, management and call routing to a set of Cisco Telepresence endpoints. *See also* endpoint.

cluster *See* server cluster.

cluster node One of the nodes in the server cluster. *See also* server cluster.

common installer A common installation script that is used to install the Cisco TelePresence Exchange System administration, database, and call engine servers. *See also* administration server, database server and call engine server.

D

database server Provides a database for configuration data and other persistent data. A pair of database servers are configured in active/standby mode. *See also* active/standby.

direct dial meeting A scheduled two-party direct dial meeting between two hosted provisioned endpoints. The Cisco TelePresence Exchange System does not reserve any media resources for a direct dial meeting. Two-party direct meetings are scheduled to provide OBTP functionality for those endpoints within the same organization. *See also* ad hoc meeting and scheduled meeting.

A scheduled two-party direct dial meeting between two hosted provisioned endpoints. The Cisco TelePresence Exchange System does not reserve any media resources for a direct dial meeting. Two-party direct meetings are scheduled to provide OBTP functionality for those endpoints within the same organization.

E

endpoint A Cisco TelePresence endpoint such as a CTS 500. Direct-dial calls are initiated between endpoints. Scheduled multipoint meetings are created by specifying the endpoints to invite.

enterprise endpoint service Enables an organization to manage the telepresence service in the enterprise network. Connectivity between organizations is provided by the service provider.

evaluation license License that is pre-installed on each Cisco TelePresence Exchange System, allowing you to operate the Cisco TelePresence Exchange System for up to 30 days. After 30 days, you must purchase a perpetual license. The evaluation license provides support for the Meet-Me service and Two-party direct dial calls. *See also* perpetual license.

F

feature-based license License that allows a specific feature, such as Meet-Me service, to function on the Cisco TelePresence Exchange System. *See also* volume-based license.

G

gateway IP address When the destination address of an IP packet is outside the local subnetwork, the packet is sent to the gateway IP address.

guest dial out An unprovisioned H.323 or ISDN endpoint that is invited to participate in a Meet-Me or Rendezvous meeting.

H

health probe Feature on the Cisco Application Control Engine that monitors the state of a server by sending messages to the server. Based on the server response, the ACE can place the server in or out of service, and can make load balancing decisions. *See also* Cisco Application Control Engine (ACE).

high availability Network design, equipment provisioning, and related software capabilities to ensure that services remain available in the event of equipment failure or network connectivity problems.

hosted endpoint service Telepresence service hosted for an organization by the service provider. The organization deploys only the telepresence endpoints. Customer endpoints register with the service provider Unified CM.

I

integrated management module (IMM) Network interface module that provides management access to the server, even if the server is powered down or is out of service. You configure the IMM before you set up and install software on the database server. *See also* database server.

interactive voice response (IVR) Feature that allows customized greetings and voice prompts to be applied to Meet-Me or Rendezvous meetings. *See also* Meet-Me meeting and Rendezvous meeting.

inter-service provider call Cisco TelePresence call that is placed between subscribers who are hosted by different service providers.

Inter-service provider direct dial with CDRs Call detail record (CDR) for direct dial calls to other service providers. The Cisco TelePresence Exchange System provides these CDRs.

intra-service provider call Cisco TelePresence call that is placed between subscribers who are hosted by the same service provider.

Intra-service provider direct dial with CDRs Call detail record (CDR) for direct dial calls between two enterprises that are hosted by the same service provider. The Cisco TelePresence Exchange System provides these CDRs.

IVR router A Cisco router that retrieves and plays all interactive voice response (IVR) files that are used by Meet-Me service meetings. The IVR router retrieves the IVR files from the call engine server. *See also* interactive voice response (IVR) and call engine server.

L

license The Cisco TelePresence Exchange System requires that a license be installed and activated for the system to operate. *See also* feature-based license, volume-based license.

load balancer Component that distributes traffic to servers in a server cluster. The Cisco Application Control Engine provides load balancing for the administration and call engine servers. *See also* administration server and call engine server.

locally-signed certificate (LSC) A certificate that is displayed when a remote user logs in by using secure shell (SSH) or hypertext transfer protocol secure (HTTPS) to validate that the user is on the correct system. This certificate is generated from information that you enter during the Cisco TelePresence Exchange System installation procedure, and it includes company name, unit, location, state, and country information for each server.

M

media resources Cisco platforms that provide capabilities for the media data path (such as multipoint switching or interactive voice response) or the media control path (such as session border controller). Media resources are grouped into clusters at a region. A resource cluster (also known as a resource pool) is a connected set of resources in one physical data center and is also known as a point of presence (POP). *See also* session border controller (SBC).

Meet-Me meeting A scheduled multipoint meeting that is hosted by the local Cisco TelePresence Exchange System to provide conferencing for two or more Cisco TelePresence or third-party endpoints. The system reserves and allocates media resources for all of the endpoints in the meeting and provides OBTP functionality to the provisioned endpoints. The system also reserves ports of organization bandwidth for the meeting, if applicable.

multipoint meeting Requires a Multipoint Control Unit (MCU) to combine or switch the media streams of the meeting participants. A multipoint meeting generally includes more than two participants.

Multipoint Control Unit (MCU) Network element that provides features for multipoint meetings. For example, the MCU can combine media streams and switch media streams between participants. The Cisco TelePresence Multipoint Switch is an example of an MCU.

N

node A single physical server in the server cluster. *See also* administration server, call engine server and database server.

O

One-Button-to-Push (OBTP) Feature that enables participants to join a Cisco TelePresence meeting with one simple action. The action may be to push a button on a video phone, or to select the meeting on the Cisco TelePresence IP phone touch-screen display. *See also* Cisco TelePresence IP phone.

organization A business customer served by a service provider. An organization controls one or more telepresence rooms (also known as endpoints) that can be included in a meeting. An organization can choose hosted endpoint service or enterprise endpoint service. *See also* hosted endpoint service and enterprise endpoint service.

P

perpetual license Permanent license that is installed on a Cisco TelePresence Exchange System and that has no expiration date. *See also* license.

point of presence (POP) Physical location of service provider resources. For the Cisco TelePresence Exchange System, the service provider POPs are data centers that house media resources (such as a Cisco TelePresence Multipoint Switch or Cisco TelePresence MSE 8000 Series) and call control resources (such as SBC).

point-to-point meeting A meeting between two Cisco TelePresence endpoints that does not require an MCU.

provisioned endpoint Endpoints for which all configuration details (such as name, phone number, number of screens, and organization) are known by the administrator and configured on the Cisco TelePresence Exchange System. If an organization has chosen hosted endpoint service, the endpoints are provisioned endpoints.

R

region Represents a major geographic area in which a service provider operates. All media resources in a region are considered to be equivalent for resource allocation purposes.

remote endpoints Endpoints for which none of the configuration details are known by the administrator. Remote endpoints are endpoints that join the meeting from another service provider network. Through the administration console, you can add remote endpoints to participate in meetings hosted by the Cisco TelePresence Exchange System.

remote meeting A Meet-Me service meeting that is hosted by a remote Cisco TelePresence Exchange System. The Cisco TelePresence Exchange System does not reserve any media resources for a remote meeting. You schedule remote meetings to provide OBTP functionality in the provisioned endpoints and to reserve ports of the organization bandwidth, if applicable.

Rendezvous meeting Also called a *timeless* or *reservationless* meeting, a Rendezvous meeting is a predefined multipoint meeting that is not limited to a single start time. For a Rendezvous meeting, the system starts a new meeting instance and allocates media bridge resources when the first participant joins the meeting. Likewise, the system deallocates resources and ends the current meeting instance when the last participant leaves the meeting.

S

scheduled meeting A meeting that starts at a future time. A scheduled meeting can be a multipoint meeting or a point-to-point meeting. *See also* multipoint meeting.

segment A unit of capacity. A segment represents one screen of video transmission. *See also* capacity.

server cluster A group of physical servers. The Cisco TelePresence Exchange System is a six-node cluster composed of two database servers, two administration servers, and a minimum of two call engine servers. *See also* database server, administration server and call engine server.

service provider An entity that offers telepresence services to a set of business customers (organizations) by using media resources that are provisioned in one or more regions of their network.

session border controller (SBC) Located at the border of a network. The SBC controls call admission to the network and protects the network from excessive call load and malicious traffic. It also provides media bridging.

The SBC includes signaling functionality managed by the Signaling Border Element (SBE), and media functionality managed by the Data Border Element (DBE). The SBC can operate in a unified or distributed deployment model. In the unified model, the SBE and DBE coexist on the same network element. In the distributed model, the SBE and DBE reside on different network elements.

session initiation protocol (SIP) A text-based call control protocol intended for creating, modifying, and terminating sessions with one or more participants. Cisco TelePresence employs SIP as the call control protocol.

static meeting A meeting that is permanently available. Each static meeting has its own associated meeting number, and meeting attendees dial that number to join the meeting.

stickiness A load balancer feature. Stickiness ensures that all messages related to one session are directed to the same server. *See also* load balancer.

system administrator A user role that can assign roles to all users and has unrestricted access to configure and modify all settings in the Cisco TelePresence Exchange System.

T

TelePresence Interoperability Protocol (TIP) Specialized protocol used by some Cisco TelePresence endpoints to provide advanced features such as multi-screen calling and spatial audio.

two-party direct A call that is a point-to-point meeting between two provisioned endpoints in the same organization. One participant initiates the meeting by direct dialing the other participant. A two-party direct call can be scheduled or ad hoc.

U

Unified CM — *See* Cisco Unified Communications Manager (Unified CM).

unprovisioned endpoint — Endpoints for which limited configuration details are known by the administrator. Through the administration console, you can add unprovisioned endpoints to participate in meetings hosted by the Cisco TelePresence Exchange System.

V

volume-based license — License that sets a limit on the number of active concurrent sessions (Cisco TelePresence meetings) that can be supported. Volume-based licenses are offered in various quantities to match the call processing requirements of the network.

INDEX

A

B

C

D

K

L

M

N

O

P

Q

R

S

T

U

V

W