



Installation and Administration Guide for the Cisco TelePresence Exchange System Release 1.0

Revised June 29, 2011

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

Text Part Number: OL-21567-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Installation and Administration Guide for the Cisco TelePresence Exchange System Release 1.0
© 2010-2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xvii

Overview of the Cisco TelePresence Exchange System

CHAPTER 1

Product Overview	1-1
Benefits	1-1
Network Architecture	1-2
Overview	1-2
Cisco TelePresence Exchange System Components	1-3
Deployment Models	1-4
Supported Features	1-4
Licensing	1-6
Key Concepts	1-6
Service Providers	1-6
Regions	1-7
Organizations	1-7
Collaboration Services	1-7
Meeting Types	1-7
Endpoint Types	1-8
Endpoint Capacity	1-8
Organization Ports Management	1-8
Session Border Controllers	1-9
Call Routing	1-9

CHAPTER 2

Overview of the Administration Console	2-1
Accessing the Administration Console	2-1
Screen Layout	2-2
Banner Pane	2-2
Navigation Pane	2-2
System Status	2-3
Content Area	2-3
Usage Guidelines	2-3
Media Resource Operational States	2-4
Common Field Properties	2-4

CHAPTER 3

Overview of the CLI 3-1

- Accessing the CLI 3-1
- Getting Help for the CLI 3-2

Installing the Cisco TelePresence Exchange System

CHAPTER 4

Preparing for Installation 4-1

- Preinstallation Checklist 4-1
- Recommendations for Rack Mounting the Cisco TelePresence Exchange System and Other Solution Components 4-2
- Power Recommendations for High Availability of the Database Servers 4-3
- Cabling Requirements 4-3
 - Cabling Requirements for the Database Servers 4-3
 - Cabling Requirements for the Administration and Call Engine Servers 4-4
- VLAN Requirements 4-5
- Gathering Required Information Before Installation 4-6
- Setting Up the IMM 4-7
 - Setting Up the IMM Network Connection 4-7
 - Creating an IMM User Account 4-8
 - Enabling SSH for the IMM 4-9

CHAPTER 5

Installing the Software 5-1

- Determining the Method and Order of Installation 5-1
 - Serial Installation 5-2
 - Parallel Installation 5-2
- Options for Connecting to the Cisco TelePresence Exchange System Servers for Installation 5-3
 - Using the IMM to Remotely Install the Cisco TelePresence Exchange System Software 5-3
- Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers 5-4
 - Installing the Database Server Software 5-4
 - Checking the Initial High-Availability Role of the Database Servers 5-8
 - Synchronizing the Database Servers 5-10
 - Verifying Synchronization and Network Connectivity of the Database Servers 5-12
- Installing the Cisco TelePresence Exchange System Call Engine Servers 5-13
 - Installing the Call Engine Server Software 5-13
 - Checking the Call Engine Server Status and Network Connectivity 5-17
- Installing the Cisco TelePresence Exchange System Administration Servers 5-18
 - Installing the Administration Server Software 5-18
 - Checking the Administration Server Status and Network Connectivity 5-22

Verifying Data Connectivity Among the Servers 5-22

CHAPTER 6
Upgrading the Software 6-1

Requirements for Upgrading the Software 6-1

Upgrading the Database Servers 6-1

Upgrading the Administration Servers and Call Engine Servers 6-3

Configuring the Cisco TelePresence Exchange System

CHAPTER 7
Getting Started with Configuration 7-1

Prerequisites for Configuring the Cisco TelePresence Exchange System 7-1

Configuration Task Sequences 7-2

Adding a Service Provider or Region 7-2

Configuring the Meet-Me Service 7-2

Configuring the Direct Dial Service 7-3

Connecting to a Remote Service Provider 7-3

Configuring Interoperability with Cisco TelePresence MSE 8000 Series 7-3

CHAPTER 8
Configuring System Settings 8-1

Understanding System Status 8-1

Live System Ping 8-2

Configuring Cluster Nodes 8-2

Editing Cluster Nodes 8-2

Deleting Cluster Nodes 8-3

Cluster Node Fields 8-3

Configuring Time Zones 8-4

Configuring Users 8-4

Adding Users 8-5

Editing User Settings 8-5

Deleting Users 8-6

User Fields 8-7

Configuring Database Backups 8-7

Retention Policy 8-8

CHAPTER 9
Configuring Media Resources 9-1

Configuring IVR Resources 9-1

Adding IVR Resources 9-1

Editing IVR Resources 9-2

- Deleting IVR Resources 9-2
- IVR Resource Fields 9-3
- Configuring SIP Resources 9-4
 - Adding SIP Resources 9-4
 - Editing SIP Resources 9-4
 - Deleting SIP Resources 9-5
 - SIP Resource Fields 9-6
- About Media Resources for Large Meetings 9-6
- Configuring CTMS Resources 9-6
 - Adding CTMS Resources 9-7
 - Editing CTMS Resources 9-7
 - Deleting CTMS Resources 9-8
 - CTMS Resource Fields 9-8
- Configuring TPS Resources 9-10
 - Adding TPS Resources 9-10
 - Editing TPS Resources 9-10
 - Deleting TPS Resources 9-11
 - TPS Resource Fields 9-11
- Configuring MSE 8510 Resources 9-13
 - Adding MSE 8510 Resources 9-13
 - Editing MSE 8510 Resources 9-13
 - Deleting MSE 8510 Resources 9-14
 - MSE 8510 Resource Fields 9-14

CHAPTER 10

Configuring Customers 10-1

- Configuring Service Providers 10-1
 - Adding Service Providers 10-1
 - Editing Service Providers 10-2
 - Deleting Service Providers 10-2
 - Service Provider Fields 10-3
- Configuring Regions 10-4
 - Adding Regions 10-4
 - Editing Regions 10-4
 - Deleting Regions 10-5
 - Region Fields 10-6
- Configuring Organizations 10-6
 - Adding Organizations 10-6
 - Editing Organizations 10-7
 - Deleting Organizations 10-7

Organization Fields 10-8

CHAPTER 11
Configuring Endpoints 11-1

- Configuring Endpoints 11-1
 - Adding Endpoints 11-2
 - Editing Endpoints 11-2
 - Deleting Endpoints 11-2
 - Endpoints Fields 11-3
- Configuring Media Profiles 11-4
 - Adding Media Profiles 11-4
 - Editing Media Profiles 11-5
 - Deleting Media Profiles 11-5
 - Media Profile Fields 11-6
- Configuring CTS Manager Resources 11-7
 - Adding CTS Manager Resources 11-7
 - Editing CTS Manager Resources 11-8
 - Deleting CTS Manager Resources 11-8
 - CTS Manager Fields 11-9

CHAPTER 12
Configuring Call Routing 12-1

- Configuring Routes 12-1
 - Adding Routes 12-1
 - Editing Routes 12-2
 - Deleting Routes 12-2
 - Route Fields 12-3
- Configuring Dial Patterns 12-4
 - Adding Dial Patterns 12-4
 - Editing Dial Patterns 12-5
 - Deleting Dial Patterns 12-5
 - Dial Patterns Fields 12-6
- Configuring Remote Service Providers 12-6
 - Adding Remote Service Providers 12-7
 - Editing Remote Service Providers 12-7
 - Deleting Remote Service Providers 12-7
 - Remote Service Provider Fields 12-8
- Viewing Call Detail Records 12-9
 - Viewing and Filtering CDRs 12-9
 - Exporting a CDR File 12-10
 - Viewing Intra-Company CDRs 12-10

Configuring Unified CM to Enable Intra-Company CDRs 12-11

CHAPTER 13

Configuring Collaboration Services 13-1

- Configuring Service Numbers 13-1
 - Adding Service Numbers 13-1
 - Editing Service Numbers 13-2
 - Deleting Service Numbers 13-2
 - Service Number Fields 13-3
- Configuring IVR Prompts 13-3
 - Adding IVR Prompts 13-4
 - Editing IVR Prompts 13-4
 - Deleting IVR Prompts 13-5
 - IVR Prompt Fields 13-5
- Scheduling Meetings 13-6
 - Viewing Meetings 13-6
 - Scheduling Meetings 13-7
 - Schedule Meeting Fields 13-8
- Scheduling Standing Meetings 13-11
 - Adding Standing Meetings 13-12
 - Editing Standing Meetings 13-12
 - Deleting Standing Meetings 13-13
 - Standing Meeting Fields 13-13

CHAPTER 14

Managing Licenses 14-1

- Viewing Licenses 14-1
- Uploading Licenses 14-2

Configuring External Network Components for Cisco TelePresence Exchange System

CHAPTER 15

Configuring the Cisco Application Control Engine 15-1

- About the Cisco Application Control Engine 15-1
 - ACE Overview 15-1
 - ACE Topology 15-1
 - Configuration Overview 15-2
- Configuring the Cisco Application Control Engine 15-3
 - Configuring the Hostname 15-4
 - Configuring Interfaces 15-5
 - Non-Redundant Configuration 15-6

Redundant Configuration	15-6
Configuring Real Servers	15-7
Configuring Access Control Lists	15-7
Configuring Health Probes	15-8
Configuring an HTTP Health Probe	15-8
Configuring a SIP Health Probe	15-9
Creating Server Farms	15-10
Configuring Session Persistence	15-11
Creating SIP Header Sticky Groups	15-11
Creating HTTP Cookie Sticky Groups	15-12
Creating HTTP Header Sticky Groups	15-13
Configuring Class Maps	15-13
Configuring Layer 7 HTTP Class Maps	15-14
Configuring Layer 7 SIP Class Maps	15-14
Configuring Layer 3 and Layer 4 Class Maps	15-15
Configuring Management Class Maps	15-15
Configuring Policy Maps	15-16
Configuring Management Policy Maps	15-16
Configuring Layer 7 Load Balancing Policy Maps	15-17
Configuring Layer 4 Policy Maps	15-18
Configuring VLAN Interfaces	15-19
Non-Redundant Configuration	15-21
Redundant Configuration	15-21
Configuring Miscellaneous Parameters	15-22
Configuring the IP Default Route	15-22
Configuring UDP Connection Timeout	15-23
Enabling SysLog SIP Messages	15-23
Configuring the Sticky Resource Class	15-23
Assigning the Admin Context to the Sticky Resource Class	15-23
Configuring ACE Logging Options	15-24

CHAPTER 16**Configuring the Cisco TelePresence Multipoint Switch 16-1**

Configuring System Settings	16-1
Configuring IP Settings	16-1
Editing Route Pattern Settings	16-2
Configuring QoS Settings	16-3
Configuring Resource Management	16-4
About SNMP Settings	16-4
Configuring Unified CM Settings	16-5

- Configuring Unified CM Settings 16-5
- Configuring SIP Profile Settings 16-6
- Configuring Cisco TelePresence Manager Settings 16-6
- Configuring Meeting Parameters 16-8
 - Configuring the Meet-Me User 16-8
 - Creating Static Meetings 16-9
 - Static Meeting Fields 16-10
- Configuring Security Settings 16-11
 - Configuring CAPF Profiles on Unified CM 16-12
 - Creating a SIP Trunk Security Profile 16-13
 - Downloading CAPF Root Certificates from Unified CM 16-14
 - Downloading Root Certificates from Unified CM 16-14
 - Uploading CAPF Certificates 16-14
 - Downloading LSC to Cisco TelePresence Multipoint Switch 16-15
 - Setting Cisco TelePresence Multipoint Switch as Secure 16-15

CHAPTER 17

Configuring the Cisco Router with IVR 17-1

- Downloading Application Files from the FTP Server 17-1
- Configuring the Router to Pass SIP Headers 17-2
- Configuring Application Parameters 17-2
- Configuring VOIP Dial Peers 17-3

CHAPTER 18

Configuring Cisco Unified Communications Manager 18-1

- Logging into the Cisco Unified Communications Manager Administration Application 18-2
- Creating a SIP Trunk Security Profile 18-2
- Creating a SIP Trunk 18-3
- Associating the SIP Trunk with Route Patterns 18-3
- Deleting a Unified CM from the Cisco TelePresence Exchange System Administration Console 18-5

CHAPTER 19

Configuring Cisco TelePresence Manager 19-1

- Configuring Lightweight Directory Access Protocol Servers 19-1
- Configuring Unified CM 19-3
 - Creating an Application User 19-3
 - Downloading the Certificate 19-4
 - Uploading the Certificate to Cisco TelePresence Manager 19-5
- Configuring the Scheduling API 19-5
- Adding Licenses 19-6

Enabling Intercompany Calls 19-7

CHAPTER 20

Configuring Cisco Session Border Controllers 20-1

Creating a Session Border Controller Interface 20-1

Creating a Management Interface 20-2

Creating the SBC Instance 20-2

Configuring the Signaling Border Element 20-3

Configuring Default Profiles 20-3

Creating Adjacencies 20-5

Configuring CAC Policy 20-7

Configuring Call Policies 20-8

Configuring SIP Timers 20-10

Defining Blacklists 20-10

Defining a Media Address 20-11

CHAPTER 21

Configuring Cisco TelePresence MSE 8000 Series 21-1

About the Cisco TelePresence MSE 8000 Series Products 21-1

Configuring Cisco TelePresence MSE 8000 Series Settings 21-2

Accessing the Web Interface 21-2

Configuring SNMP Traps 21-2

Configuring Cisco TelePresence Server MSE 8710 Settings 21-3

Configuring Services 21-3

Configuring H.323 Gatekeeper 21-4

Configuring API User 21-4

Configuring Cisco TelePresence MCU MSE 8510 Settings 21-5

Configuring Services 21-5

Configuring SNMP Traps 21-6

Configuring Conference Settings 21-6

Configuring Media Port Settings 21-6

Configuring H.323 Settings 21-7

Configuring API User 21-7

Configuring Cisco TelePresence ISDN GW MSE 8321 Settings 21-7

Configuring Services 21-8

Configuring SNMP Traps 21-8

Configuring ISDN Settings 21-8

Configuring ISDN Ports 21-9

Configuring H.323 Settings 21-9

Configuring IP to ISDN Dial Plan 21-10

Configuring Call Control 21-10

Configuring Cisco VCS Settings 21-11
 Configuring H.323 Gateway Settings on the SBC 21-11
 Configuring Adjacencies with Each Cisco VCS 21-11
 Configuring Call Policies 21-12

CHAPTER 22

Configuring Internet Group Management Protocol for Multicast Support 22-1

Multicasting Overview 22-1
 IGMP Querier 22-2
 Configuring the IGMP Querier Functionality on a Cisco Switch 22-2
 Configuring PIM on a Cisco Router 22-4
 Configuring IGMP on a Non-Cisco Switch 22-6

Maintaining the Cisco TelePresence Exchange System

CHAPTER 23

Managing Database Backups 23-1

Viewing the Scheduled Database Backup 23-1
 Viewing Past Database Server Backups and Restores 23-1
 Performing a Manual Database Backup 23-3
 Restoring a Database Server Backup 23-4

CHAPTER 24

Meeting Diagnostics 24-1

Viewing an Audit Trail 24-1
 Viewing Meeting Diagnostics (Cisco TelePresence Exchange System Release 1.0(3) and Later Only) 24-2
 Reconnecting Disconnected Meeting Participants to a Meeting (Cisco TelePresence Exchange System Release 1.0(3) and Later Only) 24-4
 Viewing Meeting Diagnostics (Cisco TelePresence Exchange System Release 1.0(2) and Earlier Only) 24-5

CHAPTER 25

Advanced Configuration 25-1

Configuring an ISDN Dial Out Prefix 25-1
 Configuring a Meet-Me External HTTP Address 25-2
 Application Parameter Fields 25-2
 Deleting an Application Parameter 25-3

CHAPTER 26

Configuring SNMP 26-1

Restrictions for SNMP 26-1
 Supported MIBs 26-2

About SNMP on the Cisco TelePresence Exchange System	26-2
Cluster Node Monitoring	26-3
Resource Monitoring	26-3
Trap Flood Mitigation	26-3
How to Configure SNMP	26-4
Adding SNMP Users	26-4
Deleting an SNMP User	26-5
Adding SNMP Trap Destinations	26-6
Removing an SNMP Trap Destination	26-7
Adding a Cluster-Identifying VIP Address to SNMP Notifications	26-8
Removing the Cluster-Identifying VIP Address from SNMP Notifications	26-10
Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB	26-10
Troubleshooting SNMP	26-12
Verifying that the SNMP Service is Running	26-12
Restarting the SNMP Service	26-13

CHAPTER 27**Configuring Cisco Discovery Protocol 27-1**

Configuring CDP	27-1
Displaying the CDP Configuration	27-2

CHAPTER 28**Changing the Network Configurations 28-1**

Changing the IP Address of an Administration or Call Engine Server	28-1
Changing the Database VIP Address That Is Configured on a Call Engine or Administration Server	28-4
Configuring SIP Load Balancing on the Call Engine Servers	28-5
Configuring the Virtual IP Address and Port for the SIP Load Balancer	28-5
Displaying the Virtual IP Address and Port for the SIP Load Balancer	28-6
Disabling SIP Load Balancing	28-6
Changing the IMM Interface Configuration	28-7

Troubleshooting the Cisco TelePresence Exchange System**CHAPTER 29****Password Recovery 29-1****CHAPTER 30****Split Brain Recovery 30-1**

Diagnosing Split Brain Mode	30-1
Recovering from Split Brain Mode	30-3
Verifying Synchronization of the Database Servers	30-4
Diagnosing Corrupted DRBD Metadata	30-6

Recovering from Corrupted DRBD Metadata 30-7

CHAPTER 31

Corrupted MySQL Database Recovery 31-1

Diagnosing a Corrupted MySQL Database 31-1

Recovering from a Corrupted MySQL Database 31-2

CHAPTER 32

Troubleshooting Calls 32-1

Troubleshooting Interop Calls 32-1

Troubleshooting an Interop Call in Cisco TelePresence Exchange System Release 1.0(3) and Later 32-1

Troubleshooting an Interop Call in Cisco TelePresence Exchange System Release 1.0(2) 32-2

Troubleshooting Failure of an Endpoint to Call into a Second Meeting 32-4

CHAPTER 33

Server Failure Recovery 33-1

Recovering from a Failed Primary Database Server 33-1

Disabling High Availability to Enable the Current Secondary Database Server to Take Over the Primary Role 33-1

Enabling HA After Recovering a Database Server 33-3

Replacing a Database Server 33-4

Preparing to Replace a Database Server 33-4

Setting Up the Replacement Database Server 33-5

Installing the Software on and Synchronizing the Replacement for the Initial Secondary Database Server 33-6

Installing the Software on and Synchronizing the Replacement for the Initial Primary Database Server 33-7

Replacing an Administration or Call Engine Server 33-9

CHAPTER 34

Logs 34-1

Obtaining Logs for a Customer Service Representative 34-1

Appendixes

APPENDIX A	Installation Worksheets	A-1
APPENDIX B	Endpoint Capacity	B-1
APPENDIX C	Command Reference	C-1
APPENDIX D	MIB Reference	D-1
	CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB	D-1
	Update Intervals for SNMP Tables	D-1
	Overall Health System Status Objects	D-2
	Table Objects	D-3
	Trap Notification Objects	D-5
	Read-Write Objects	D-8
	Configuration Tasks for the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB	D-10
GLOSSARY		



Preface

Revised June 29, 2011

This preface contains the following sections:

- [Audience](#)
- [Purpose](#)
- [Organization](#)
- [Conventions](#)
- [Related Publications](#)
- [Obtaining Documentation and Submitting a Service Request](#)

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 and product-specific MIBs.
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 .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	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.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	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 Publications

For more information about the Cisco TelePresence Exchange System, go to:

<http://www.cisco.com/go/ctx-docs>

The following documents describe Cisco TelePresence products and other platforms that are related to the Cisco TelePresence Exchange System:

- Cisco TelePresence Manager:
http://www.cisco.com/en/US/products/ps7074/tsd_products_support_series_home.html
- Cisco TelePresence Multipoint Switch:
http://www.cisco.com/en/US/products/ps7315/tsd_products_support_series_home.html
- Cisco Application Control Engine appliance:
http://www.cisco.com/en/US/products/ps6021/tsd_products_support_series_home.html
- Cisco Unified Communications Manager:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- Cisco TelePresence MSE 8000 Series:
http://www.cisco.com/en/US/products/ps11340/tsd_products_support_series_home.html
- Cisco ASR 1000 Series Aggregation Services Router documentation
http://www.cisco.com/en/US/products/ps9343/tsd_products_support_series_home.html

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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.



PART 1

Overview of the Cisco TelePresence Exchange System

- [Product Overview](#)
- [Overview of the Administration Console](#)
- [Overview of the CLI](#)



CHAPTER 1

Product Overview

Revised June 29, 2011

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 new services production 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, page 1-1](#)
- [Network Architecture, page 1-2](#)
- [Supported Features, page 1-4](#)
- [Licensing, page 1-6](#)
- [Key Concepts, page 1-6](#)

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.

Network Architecture

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

- [Overview, page 1-2](#)
- [Cisco TelePresence Exchange System Components, page 1-3](#)
- [Deployment Models, page 1-4](#)

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 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](#), at <http://www.cisco.com/go/ctx-relnotes>.

- 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 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 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 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 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 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 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 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.

Supported Features

The Cisco TelePresence Exchange System supports the features that are listed in [Table 1-1](#).

Table 1-1 Supported Features

Feature	Description
Meet-Me service	<p>The Meet-Me service provides conferencing for two or more Cisco TelePresence or third-party endpoints and includes the following functionality:</p> <ul style="list-style-type: none"> • The scheduling API provides web services to schedule and manage Meet-Me meetings. • Cisco TelePresence Exchange System provides automated One-Button-to-Push (OBTP) functionality for hosted endpoints. • The Cisco TelePresence Exchange System monitors Cisco TelePresence Multipoint Switch operational status, to ensure that new meetings are scheduled using only operational Cisco TelePresence Multipoint Switch units. In addition, the Cisco TelePresence Exchange System monitors the operational status of the Cisco TelePresence MSE 8000 Series. • An integrated IVR application provides greetings and voice prompts for the conference participants. Service Providers can install branded voice prompt files. • Cisco TelePresence Exchange System reserves the appropriate meeting resource (Cisco TelePresence Multipoint Switch or Cisco MSE 8000 Series) capacity for each meeting when it is scheduled. • Cisco TelePresence Exchange System prevents additional participants from joining a meeting if the meeting is already using its maximum capacity.

Table 1-1 Supported Features (continued)

Feature	Description
Two-party direct dial calls	<p>Cisco TelePresence Exchange System supports ad-hoc and scheduled direct dial calls between two endpoints in the same organization. The Cisco TelePresence Exchange System does not reserve any media resources for direct dial calls.</p> <p>A two-party direct dial meeting can be scheduled only between two provisioned endpoints, and the two endpoints must be associated with a CTS-Manager. The value of scheduling the meeting is to provide OBTP functionality for the endpoints.</p> <p>Ad-hoc direct dial calls can be between any two endpoints in the organization. For a description of endpoint types, see the “Endpoint Types” section on page 1-8.</p>
Scheduling API	The 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 meetings and two-party meetings.
Call Detail Records (CDR) API	The CDR API provides services to retrieve call detail records from the Cisco TelePresence Exchange System.
Management, monitoring, and provisioning	The administration console provides web-based administration and configuration for the Cisco TelePresence Exchange System.
Carrier-grade availability and scalability	<p>The Cisco TelePresence Exchange System incorporates the following high-availability features:</p> <ul style="list-style-type: none"> • 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.
Support for Cisco TelePresence MSE 8000 Series	<p>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.</p> <p>The Cisco TelePresence Exchange System uses the following types of service modules:</p> <ul style="list-style-type: none"> • Cisco TelePresence MCU MSE 8510—Provides inter-working with single-screen standards-based telepresence endpoints that support either the 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.
Guest Dial Out	Allows any unprovisioned H.323 or ISDN endpoint to participate in a Meet-Me conference.

Table 1-1 Supported Features (continued)

Feature	Description
Support for 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, even if the resources span multiple POPs.
Inter-company direct dial with call detail records (CDRs)	The Cisco TelePresence Exchange System provides CDRs for direct dial calls between two enterprises that are hosted by the same service provider.
Inter-service provider direct dial with CDRs	The Cisco TelePresence Exchange System provides CDRs for direct dial calls to other service providers.

Licensing

The Cisco TelePresence Exchange System requires the installation of a license to enable Meet-Me and direct dial services. The system checks the license before scheduling a meeting or initiating a Meet-Me 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 30-day evaluation license. After 30 days, you must install a permanent license to continue to use the Meet-Me 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.

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 1-7](#)
- [Organizations, page 1-7](#)
- [Collaboration Services, page 1-7](#)
- [Meeting Types, page 1-7](#)
- [Endpoint Types, page 1-8](#)
- [Endpoint Capacity, page 1-8](#)
- [Organization Ports Management, page 1-8](#)
- [Session Border Controllers, page 1-9](#)
- [Call Routing, page 1-9](#)

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).

All media resources in a region are considered to be equivalent for resource allocation purposes, even if the resources span multiple POPs.

All media resources in a region are dedicated to one service provider.

A service provider might have multiple regions configured on a Cisco TelePresence Exchange System.

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.

Collaboration Services

You can define the following collaboration services on the Cisco TelePresence Exchange System: meetings, standing meetings, IVR prompts, and service numbers.

There is a set of pre-defined meeting types that the service provider can configure. For more information, see the [“Meeting Types” section on page 1-7](#).

The service number is the number that users dial to reach the service such as Meet-Me. You must configure at least one service number for each service provider on the Cisco TelePresence Exchange System.

The service number configuration specifies the associated IVR prompts files. This enables the service provider to configure multiple service numbers for a service, each one with a different set of voice prompts.

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. 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 bandwidth for the meeting, if requested.
- **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 the bandwidth, if requested.

- **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 dialed 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.

Endpoint Types

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. Meet-Me and direct dial calls are placed on provisioned endpoints.
- **Unprovisioned endpoints**—Endpoints for which none of the configuration details are known by the administrator except the name of the meeting scheduler for the endpoint. Through the administration console you can reserve bandwidth for unprovisioned endpoints on the service provider network. This allows the endpoint to connect with other known endpoints within the network that are scheduled for the same meeting. This capability is useful for intercompany meetings.
- **Remote endpoints**—Endpoints for which no configuration details are known. Remote endpoints are endpoints that join the meeting from another service provider network. Configuring a remote endpoint on the Cisco TelePresence Exchange System reserves capacity for the endpoint on the service provider network on which it is resident. The Cisco TelePresence Exchange System automatically determines and reserves the capacity to support these interprovider meetings.

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 beginning with Cisco TelePresence Exchange System Release 1.0(3), you can specify either that the smallest amount of capacity possible will be reserved for endpoints, or the maximum capacity per endpoint, depending on your needs.

For more details on endpoint capacity calculation, see the [“Endpoint Capacity”](#) appendix.

Organization Ports Management

Organization ports management 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.

You specify the maximum number of ports when you configure an organization. The units are segments (screens). The ports required for each endpoint are specified in the endpoint table. You must specify the ports that are required by endpoints when you schedule the meeting.

When the system schedules a 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 maximum value (for all meetings that are scheduled in the time slot), the system rejects the attempt to schedule this meeting.

Session Border Controllers

The session border controller (SBC) is 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. The SBC 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 operates in the unified deployment model, which means that the SBE and DBE coexist on same network element.

The SBC controls adjacencies, which represent a signaling relationship with a remote call agent. There is one adjacency defined per external 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 a second adjacency.

The Cisco TelePresence Exchange System connects to SIP endpoints by using an SBC that supports the SIP protocol, and connects to H.323 endpoints by using an SBC that supports the H.323 protocol. A single SBC can support both the SIP and H.323 protocol.

Call Routing

On the Cisco TelePresence Exchange System, a route is a reference to an adjacency on an SBC. Each adjacency on the SBC is assigned a unique tag. The tag value is included in SIP messages between the SBC and Cisco TelePresence Exchange System, which simplifies routing.

For example, the SBC has an adjacency for each enterprise Cisco Unified Communications Manager. The adjacency is configured with a unique tag. The same tag value is configured in the Cisco TelePresence Exchange System route for that organization. The outgoing route on the SBC is found by matching the tag value in the SIP message.



CHAPTER 2

Overview of the Administration Console

Revised June 29, 2011

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, page 2-1](#)
- [Screen Layout, page 2-2](#)
- [Usage Guidelines, page 2-3](#)
- [Media Resource Operational States, page 2-4](#)
- [Common Field Properties, page 2-4](#)

Accessing the Administration Console

You can access the administration console from any computer that can connect to the external IP address of 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, page 2-2](#)
- [Navigation Pane, page 2-2](#)
- [System Status, page 2-3](#)
- [Content Area, page 2-3](#)

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.
- **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.
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).

Table 2-1 *Navigation Categories (continued)*

Category	Description
Collaboration Services	Configuring meetings, service numbers, and IVR prompts.
Licensing	Managing licenses.
Diagnostics	Viewing meeting diagnostics and event audit trails.
Advanced Configuration	Defines the external HTTP load-balancing address for the call engines when an ACE is in use within the network, and defines the ISDN dial out prefixes.

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 7.x and later
 - Mozilla Firefox versions 3 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).

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. 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. 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 a 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.
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.



CHAPTER 3

Overview of the CLI

Revised June 29, 2011

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, page 3-1](#)
- [Getting Help for the CLI, page 3-2](#)

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 username **admin** to log in to the CLI. The password for the admin user was defined during server 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 database*
      utils service list
      utils service sipserver*
      utils service start
      utils service stop
```

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

```
admin: help utils service list

service list help:
This will retrieve all services status

options are:
page      - pause output
```

```
Example:
admin:utils service list
System NTP [STARTED]
System SSH [STARTED]
....
```

- For details about each command, see [Appendix C, “Command Reference.”](#)



PART 2

Installing the Cisco TelePresence Exchange System

- [Preparing for Installation](#)
- [Installing the Software](#)
- [Upgrading the Software](#)



CHAPTER 4

Preparing for Installation

Revised June 29, 2011

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

- [Preinstallation Checklist, page 4-1](#)
- [Recommendations for Rack Mounting the Cisco TelePresence Exchange System and Other Solution Components, page 4-2](#)
- [Power Recommendations for High Availability of the Database Servers, page 4-3](#)
- [Cabling Requirements, page 4-3](#)
- [VLAN Requirements, page 4-5](#)
- [Gathering Required Information Before Installation, page 4-6](#)
- [Setting Up the IMM, page 4-7](#)

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. Cisco recommends that you use an uninterruptible power supply (UPS) or dual power sources, especially for the database servers. See the “Power Recommendations for High Availability of the Database Servers” section on page 4-3.	
Check that the servers are properly cabled. See the “Cabling Requirements” section on page 4-3.	
Check that you can access the Cisco TelePresence Exchange System servers (database, administration, and call engine) by using a local console.	

Preinstallation Tasks	Checkoff
<p>Check that you have one of the following browsers for configuring and using the integrated management module (IMM):</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer version 6.0 or later with the latest Service Pack • Mozilla Firefox version 1.5 or later 	
<p>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.</p>	
<p>Verify that you have all the required information before you begin the installation. See the “Gathering Required Information Before Installation” section on page 4-6.</p>	
<p>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.</p>	
<p>Specifically for the database servers, if you use separate VLANs for the system management network (IMM) and data network (Ethernet 0 and Ethernet 2), make sure that packets can be routed between the separate VLANs.</p>	
<p>Verify that each VLAN that will have a Cisco TelePresence Exchange System server can connect to the NTP servers.</p>	
<p>Set up the IMM for each database server and, optionally, each call engine and administration server. See the “Setting Up the IMM” section on page 4-7.</p>	

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.

Power Recommendations for High Availability of the Database Servers

In order for the high availability (HA) implementation to work properly for the database servers, each database server must be able to reach the integrated management module (IMM) of the peer database server. If the IMM of the primary database server is unreachable by the secondary database server, and the primary database server fails, the secondary database server cannot take over the primary role. In this situation, all calls to or from the system fail, and meetings cannot be scheduled or modified. To recover from this situation, see the [“Recovering from a Failed Primary Database Server”](#) section on page 33-1.

Because power loss causes the server and its IMM to fail, make sure that both power cords are securely attached to each database server. Also, Cisco recommends that you take at least one of the following actions to prevent power loss to the database servers:

- Connect each power cord to an independent power supply, so that each database server has dual power sources.
- Use an uninterruptible power supply (UPS) to prevent power loss to each database server.

The IMM of the peer database server may also become unreachable due to network issues. Therefore, ensure reliable network connectivity between the database servers by connecting the cables as specified in the [“Cabling Requirements for the Database Servers”](#) section on page 4-3.

Cabling Requirements

- [Cabling Requirements for the Database Servers, page 4-3](#)
- [Cabling Requirements for the Administration and Call Engine Servers, page 4-4](#)

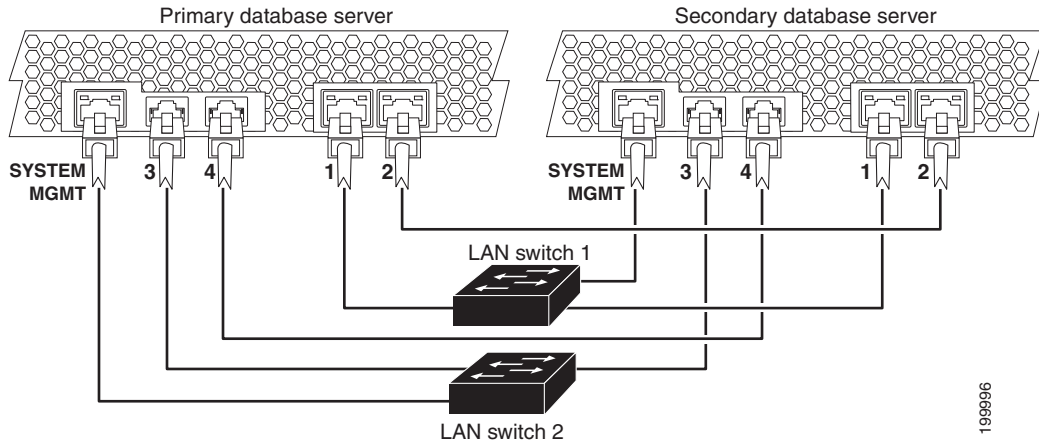
Cabling Requirements for the Database Servers

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
SYSTEM MGMT	Integrated management module (IMM)	—
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

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

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

In each server, Ethernet 0 and Ethernet 1 are on one NIC, while Ethernet 3 and Ethernet 4 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.

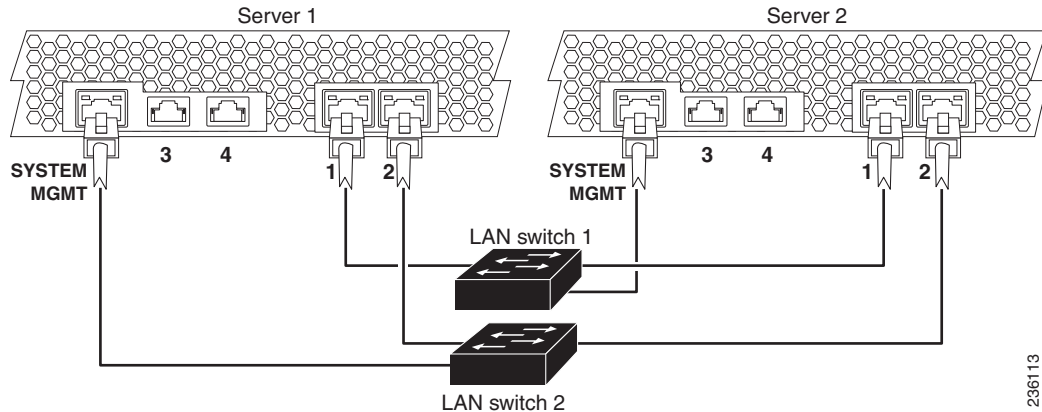
Cabling Requirements for the Administration and Call Engine Servers

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

236113

Port label	Interface	Bonded Interface
SYSTEM MGMT	Integrated management module (IMM)	—
1	Ethernet 0—data	Bond 0
2	Ethernet 1—data	Bond 0
3	Ethernet 2—currently not used	—
4	Ethernet 3—currently not used	—

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.

Cisco recommends that you connect the IMM interfaces to separate LAN switches.

VLAN Requirements

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

- The following requirements apply to the data network interfaces of the Cisco TelePresence Exchange System:
 - Ethernet 0 and Ethernet 2 of both database servers must be on the same VLAN.
 - Ethernet 0 and Ethernet 1 of both administration servers and both call engine servers must be on the same VLAN.
 - You may use the same VLAN for the data network interfaces of all nodes in the Cisco TelePresence Exchange System server cluster.
- The data VLAN of the Cisco TelePresence Exchange System call engine servers 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)

- Cisco recommends that you use a separate system management VLAN for the integrated management module (IMM) interfaces on the Cisco TelePresence Exchange System servers.

**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” 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.
 - One IP address for each integrated management module (IMM) interface.

The two database servers are the only servers that require configured IMM interfaces, but you may want to configure the IMM interfaces on the call engine and administration servers to enable remote control of those servers.

- IP address of the default gateway for each server and IMM interface.
- Administrator usernames and passwords:
 - For accessing the CLI of each database, administration, and call engine server. To simplify management, Cisco recommends that you use the same username and password on all Cisco TelePresence Exchange System servers.
 - For accessing each IMM interface. The two database servers are the only servers that require configured IMM interfaces, but you may want to configure the IMM interfaces on the call engine and administration servers to enable remote control of the servers.
- 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 must set up the IMM on the database servers before you install the Cisco TelePresence Exchange System software. The IMM is required to implement active/standby redundancy for the two database servers.

You may also choose to set up the IMM on the administration and call engine servers to enable you to control those servers 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: **PASSWORD** (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:
- In the Login Profiles area, click the **USERID** Login ID.
 - Enter a new password into the **Password** and **Confirm password** fields.
 - 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.
-



CHAPTER 5

Installing the Software

Revised June 29, 2011

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

- [Determining the Method and Order of Installation, page 5-1](#)
- [Options for Connecting to the Cisco TelePresence Exchange System Servers for Installation, page 5-3](#)
- [Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers, page 5-4](#)
- [Installing the Cisco TelePresence Exchange System Call Engine Servers, page 5-13](#)
- [Installing the Cisco TelePresence Exchange System Administration Servers, page 5-18](#)
- [Verifying Data Connectivity Among the Servers, page 5-22](#)

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:

- [Serial Installation, page 5-2](#)
- [Parallel Installation, page 5-2](#)

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

Installation Method	Advantage	Disadvantage
Serial	<p>Less opportunity for entry errors.</p> <p>You enter information into the installation wizard for only one server at a time.</p>	<p>Longer installation process.</p> <p>Each server installation requires 40 minutes to install. So the full serial installation requires 240 minutes (6 servers × 40 minutes each).</p>
Parallel	<p>Shorter installation process.</p> <p>Each server pair requires 40 minutes to install. You must install the database servers before you begin to install the administration and call engine servers.</p> <p>Depending on whether you install all four of the administration and call engine servers at the same time, the full parallel installation requires one of the following lengths of time:</p> <ul style="list-style-type: none"> • 120 minutes (3 parallel installations × 40 minutes) • 80 minutes (2 parallel installations × 40 minutes) 	<p>Greater opportunity for entry errors.</p> <p>You enter information into the installation wizard for two to four servers at a time.</p>

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 5-13
- [Installing the Cisco TelePresence Exchange System Administration Servers](#), page 5-18

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 the servers in parallel in the following order:

1. Install the primary and secondary database servers in parallel.

Ensure that the database server installations and synchronization are complete before you proceed to install the call engine and administration servers.

2. 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 5-13
- [Installing the Cisco TelePresence Exchange System Administration Servers](#), page 5-18

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 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 your 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.

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 5-13](#)
- [Installing the Cisco TelePresence Exchange System Administration Servers, page 5-18](#)

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 Role of the Database Servers, page 5-8](#)
- [Synchronizing the Database Servers, page 5-10](#)
- [Verifying Synchronization and Network Connectivity of the Database Servers, page 5-12](#)

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.

**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 **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 **Yes** or **No**, depending on whether you want to enable the Domain Name Server (DNS) client on the database server.

If you select **Yes**, complete the following steps in the DNS Client Configuration screen:

- a. Enter the IP address for the primary DNS server.
- b. (Optional) Enter the IP address for the secondary DNS server.
- c. Enter the DNS domain name, for example, “cisco.com” or “example.net.”
- d. Select **OK**.



Note If you enable the DNS client, make sure that the DNS servers have entries for each hostname and IP address pair, including the virtual hostname and VIP address that are shared by the database servers. During the installation process, the DNS client connects to the DNS server to resolve the hostname and IP address that you entered in [Step 6](#).

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 IP address, username, and password for the IMM interface.
- d. Enter the VIP address to be shared by the primary and secondary database servers.
- e. Select **OK**.
- f. Enter the following information for the *peer* server.
 - IMM IP address, username, and password for the peer server.
 - Hostname and IP address of the peer server.



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

- g. 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:

- a. In the Administrator ID field, enter a username.
- b. In the Password and Confirm Password fields, enter a password.
- c. Select **OK**.

You can use the same username and password for all database, administration, and call engine servers.

- 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 Role of the Database Servers”](#) section on page 5-8.

Checking the Initial High-Availability Role of the Database Servers

Complete this task on each database server to confirm the correct initial high-availability (HA) role of primary or secondary.

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
Unable to run CLI as root due to unsuccessful service drbd status!
-----
The initial configured HA role of this node      : primary
The current HA role of this node                 :
The database vip address                         : 10.22.130.54
The database primary node name                   : ctx-db-1
The database primary node IP address             : 10.22.130.49
The database secondary node name                 : ctx-db-2
```

```

The database secondary node IP address      : 10.22.130.57
Unable to run CLI as root due to unsuccessful service heartbeat status!
Mon status                                 : Not running (only runs on primary)
MySQL status                               : Not running (only runs on primary)
Heartbeat status                           : Not running
-----
-----

```

Executed command unsuccessfully

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

```

admin: utils service database status
Unable to run CLI as root due to unsuccessful service drbd status!
-----
The initial configured HA role of this node      : secondary
The current HA role of this node                 :
The database vip address                         : 10.22.130.54
The database primary node name                   : ctx-db-1
The database primary node IP address             : 10.22.130.49
The database secondary node name                 : ctx-db-2
The database secondary node IP address          : 10.22.130.57
Unable to run CLI as root due to unsuccessful service heartbeat status!
Mon status                                       : Not running (only runs on primary)
MySQL status                                    : Not running (only runs on primary)
Heartbeat status                                : Not running
-----
-----

```

Executed command unsuccessfully



Note

Because the database servers have not yet been synchronized, you may notice the following information in the output:

- The current HA role of each node is blank.
- The Distributed Replicated Block Device (DRBD) feature is not yet available. This feature synchronizes the secondary database with changes that are made on the primary database.
- The heartbeat is not yet running.
- The system reports that it executed the command unsuccessfully.

What to Do Next

Proceed to the [“Synchronizing the Database Servers”](#) section on page 5-10.

Related Topics

- [Appendix C, “Command Reference”](#)

Synchronizing the Database Servers

When you initiate database synchronization, you enable the heartbeat connection, begin running MySQL (on the primary database server only), and synchronize the data between the two database servers.

Before You Begin

Complete these tasks for both database servers:

- [Installing the Database Server Software, page 5-4](#)
- [Checking the Initial High-Availability Role of the Database Servers, page 5-8](#)

Procedure

-
- Step 1** Log in to the CLI of the database server that was initially configured with the *primary* HA role.
- Step 2** Enter the **utils service database sync** command to set up synchronization on the initial primary server. The synchronization takes approximately 10 minutes and includes a reboot of the secondary database server.
- Step 3** Enter the **utils service database status** command to check the synchronization status of the initial primary server.

After the synchronization process is complete on the initial primary server, the command output will indicate the following items:

- The server currently has the *primary* HA role.
- The heartbeat is running.
- The connection state (cs) of WfConnection, which is short for “waiting for a connection,” indicates that the primary server is waiting for the secondary server to become available on the network.

For example:

```
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
The database primary node name                 : ctx-db-1
The database primary node IP address          : 10.22.130.49
The database secondary node name              : ctx-db-2
The database secondary node IP address        : 10.22.130.57
Mon status                                     : Running pid 1527
MySQL status                                  : Running pid 1472
Heartbeat status                             : Running pid 32570
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res  cs          ro          ds          p  mounted  fstype
0:mysql WfConnection Primary/Unknown UpToDate/DUnknown C /mnt/mysql ext3
-----
```

- Step 4** Log in to the CLI of the database server that was initially configured with the *secondary* HA role.
- Step 5** Enter the **utils service database sync** command to set up synchronization on the initial secondary server.

Step 6 Enter the **utils service database status** command on both database servers to check the synchronization status.

Synchronization between the database servers takes approximately 40 minutes. During that time, the disk state (ds) of the secondary server is shown as **inconsistent**. An inconsistent state indicates that the synchronization between the primary and secondary servers is not complete. The synchronization progress appears as a percentage in the command output.

Sample output from a 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
The database primary node name                    : ctx-db-1
The database primary node IP address              : 10.22.130.49
The database secondary node name                  : ctx-db-2
The database secondary node IP address            : 10.22.130.57
Mon status                                        : Running pid 1527
MySQL status                                      : Running pid 1472
Heartbeat status                                  : Running pid 32570
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res  cs          ro          ds          p mounted  fstype
...    sync'ed:  11.0%          (41060/46080)M
0:mysql SyncSource Primary/Secondary UpToDate/Inconsistent C /mnt/mysql ext3
-----
```

Sample output from a 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
The database primary node name                    : ctx-db-1
The database primary node IP address              : 10.22.130.49
The database secondary node name                  : ctx-db-2
The database secondary node IP address            : 10.22.130.57
Mon status                                        : Not running (only runs on primary)
MySQL status                                      : Not running (only runs on primary)
Heartbeat status                                  : Running pid 1581
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res  cs          ro          ds          p mounted  fstype
...    sync'ed:  11.0%          (41032/46080)M
0:mysql SyncTarget Secondary/Primary Inconsistent/UpToDate C
-----
```

What to Do Next

Proceed to the [“Verifying Synchronization and Network Connectivity of the Database Servers”](#) section on page 5-12.

Related Topics

- [Appendix C, “Command Reference”](#)

Verifying Synchronization and Network Connectivity of the Database Servers

Before You Begin

Complete the task in the “[Synchronizing the Database Servers](#)” section on page 5-10.

Procedure

- Step 1** To verify that synchronization is complete, enter the **utils service database status** command on both database servers.

When synchronization is complete, the output includes the following status:

- The role (ro) values indicate that each server recognizes the correct current HA roles for itself (value on the left) and its peer (value on the right).
- The disk state (ds) values indicate that each server sees itself and its peer as being up to date.

Sample output from a 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
The database primary node name                 : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name               : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Running pid 1527
MySQL status                                   : Running pid 1472
Heartbeat status                               : Running pid 32570
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res    cs          ro          ds          p  mounted  fstype
0:mysql  Connected    Primary/Secondary UpToDate/UpToDate C  /mnt/mysql ext3
-----
```

Sample output from a 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
The database primary node name                 : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name               : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Not running (only runs on primary)
MySQL status                                   : Not running (only runs on primary)
Heartbeat status                               : Running pid 1581
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res    cs          ro          ds          p  mounted  fstype
0:mysql  Connected    Secondary/Primary UpToDate/UpToDate C
-----
```

- Step 2** To verify network connectivity, 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
```

Troubleshooting Tips

If the **utils service database status** command output differs from what is described in the procedure, your system may be in split brain mode. See the “[Split Brain Recovery](#)” section on page 30-1.

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 5-13](#)
- [Checking the Call Engine Server Status and Network Connectivity, page 5-17](#)

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.

**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:
- Enter the host name, IP address, and subnet mask for the call engine server.
 - Enter the IP address for the default gateway.
 - Select **OK**.
- Step 8** In the DNS Client Configuration screen, select **Yes** or **No**, depending on whether you want to enable the Domain Name Server (DNS) client on the database server.



Note If you enable the DNS client, make sure that the DNS servers have entries for each hostname and IP address pair, including the virtual hostname and VIP address that are shared by the database servers. During the installation process, the DNS client connects to the DNS server to resolve the hostname and IP address that you entered in [Step 7](#).

Only if you select **Yes**, complete the following steps in the DNS Client Configuration screen:

- Enter the IP address for the primary DNS server.
 - (Optional) Enter the IP address for the secondary DNS server.
 - Enter the DNS domain name, for example, “cisco.com” or “example.net.”
 - Select **OK**.
- 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:
- IP Address—Enter the VIP address of the ACE.
 - Port—Enter the port number on which the call engine server will connect to the load balancer.
 - 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:
- Enter a username in the Administrator ID field.
 - Enter a password into the Password and Confirm Password fields.
 - Select **OK**.

Cisco recommends that you use the same username and password for all database, administration, and call engine servers.

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 5-17.

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 5-18](#)
- [Checking the Administration Server Status and Network Connectivity, page 5-22](#)

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 5-13.
- 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.



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 **Yes** or **No**, depending on whether you want to enable the Domain Name Server (DNS) client on the database server.

Only if you select **Yes**, complete the following steps in the DNS Client Configuration screen:

- a. Enter the IP address for the primary DNS server.
- b. (Optional) Enter the IP address for the secondary DNS server.
- c. Enter the DNS domain name, for example, “cisco.com” or “example.net.”
- d. Select **OK**.



Note If you enable the DNS client, make sure that the DNS servers have entries for each hostname and IP address pair, including the virtual hostname and VIP address that are shared by the database servers. During the installation process, the DNS client connects to the DNS server to resolve the hostname and IP address that you entered in [Step 7](#).

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:

- a. Enter a username in the Administrator ID field.
- b. Enter a password into the Password and Confirm Password fields.
- c. Select **OK**.

You can use the same username and password for all database, administration, and call engine servers.

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 5-22.

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:
- Repeat [Step 1](#), but this time use the IP address of the *other* administration server.
If the login page appears, proceed to [Step 3](#).
 - Make sure that the browser machine can reach other devices in the same VLAN as the administration servers. Resolve any network connectivity issues.
 - The administration server may be configured with an incorrect VIP address for the database servers. Complete the procedure in the “[Changing the Database VIP Address That Is Configured on a Call Engine or Administration Server](#)” section on page 28-4.
 - Repeat [Step 1](#).
 - If you still cannot reach the admin console, the security password that you entered while installing the administration server does not match the security password that you entered while installing the the initial primary database server.

To change the security password on a server, you need to reinstall that server. See the “[Installing the Cisco TelePresence Exchange System Administration Servers](#)” section on page 5-18.

If reinstalling to change the security password on the administration server does not enable you to reach the admin console, you need to reinstall and change the security password on both database servers. See the “[Installing and Synchronizing the Cisco TelePresence Exchange System Database Servers](#)” section on page 5-4.
- 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 5-13
 - [Installing the Cisco TelePresence Exchange System Administration Servers](#), page 5-18
-



CHAPTER 6

Upgrading the Software

Revised June 29, 2011

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

- [Requirements for Upgrading the Software, page 6-1](#)
- [Upgrading the Database Servers, page 6-1](#)
- [Upgrading the Administration Servers and Call Engine Servers, page 6-3](#)

Requirements for Upgrading the Software

- Cisco strongly recommends that all six nodes in the server cluster run the exact same software version. Nevertheless, the system is designed to support the following requirements:
 - Each database server must run the exact same software version as its peer database server.
 - Each administration server and call engine server must run the exact same software version as the other administration and call engine servers in the cluster.

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>.

- If you plan to upgrade all six nodes, which Cisco recommends, then upgrade the database servers before you upgrade the administration and call engine servers.

Upgrading the Database Servers

Before You Begin

- Read the “[Requirements for Upgrading the Software](#)” section on page 6-1.
- The database server upgrade process requires a scheduled maintenance window of system downtime, because you need to back up the database, shut down the database servers to install the new software, restore the database, and then synchronize the database servers. Minimum required maintenance windows are as follows:
 - For a parallel installation (which means that you install the new software on both database servers at the same time), you will need at least 3 hours of system downtime.

- For a serial installation (which means that you complete the installation on one database server before you begin the installation on the other database server), you will need at least 4 hours of system downtime.



Note If you plan to also upgrade all the other Cisco TelePresence Exchange System nodes, Cisco recommends that you extend your maintenance period by 3 hours. You will also need to confirm that a Cisco customer support representative is available during your planned maintenance period to perform the upgrade procedure for your administration and call engine servers. See the “[Upgrading the Administration Servers and Call Engine Servers](#)” section on page 6-3.

Schedule the maintenance period and notify all users about your system downtime. If possible, block users from scheduling meetings that will occur during this maintenance period.

- 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>.

Procedure

-
- Step 1** From the administration console, back up the database.
For instructions, see the “[Performing a Manual Database Backup](#)” section on page 23-3.
- Step 2** Stop the administration and call engine servers:
- Enter the `utils service adminserver stop` command in the CLI of each administration server.
 - Enter the `utils service sipserver stop` command in the CLI of each call engine server.
- Step 3** Shut down both database servers by entering the `utils system shutdown` command in the CLI of each database server.
- Step 4** Install the new software on the database servers by completing these tasks:
- [Installing the Database Server Software, page 5-4](#)
 - [Checking the Initial High-Availability Role of the Database Servers, page 5-8](#)
- Step 5** Synchronize the database servers by completing these tasks:
- [Synchronizing the Database Servers, page 5-10](#)
 - [Verifying Synchronization and Network Connectivity of the Database Servers, page 5-12](#)
- Step 6** If you had planned to upgrade all Cisco TelePresence Exchange System nodes in the server cluster during this maintenance period, then contact the Cisco customer service representative now to upgrade the administration and call engine servers for you.
Whether or not the administration and call engine servers were upgraded, proceed to the next step.
- Step 7** Start the administration and call engine servers:
- Enter the `utils service adminserver start` command in the CLI of each administration server.
 - Enter the `utils service sipserver start` command in the CLI of each call engine server.
- Step 8** From the administration console, restore the database by using the backup from [Step 1](#).
For instructions, see the “[Restoring a Database Server Backup](#)” section on page 23-4.

**Note**

To log in to the administration console, use the default username **admin** and password **cisco**. After the database is restored, you can log in with the username and password that you used before beginning this upgrade procedure.

- Step 9** Complete the procedure in the “[Verifying Data Connectivity Among the Servers](#)” section on page 5-22.
- Step 10** Close the maintenance window and notify your users that they may now use the system.

Related Topics

- [Command Reference, page C-1](#)

Upgrading the Administration Servers and Call Engine Servers

Before You Begin

Read the “[Requirements for Upgrading the Software](#)” section on page 6-1.

Procedure

- Step 1** Contact a Cisco customer service representative to schedule a time to upgrade the administration and call engine servers.
- Step 2** Schedule a maintenance window of 3 hours to begin at the time you scheduled in [Step 1](#).
- Notify all users about your system downtime.
 - If possible, block users from scheduling meetings that will occur during this maintenance period.
- Step 3** At the scheduled time for the administration and call engine server upgrades, contact the Cisco customer service representative, who will upgrade those servers for you.
- Step 4** When the Cisco customer service representative confirms that the upgrades are complete, close the maintenance window and notify your users that they may now use the system.

Related Topics

- [Upgrading the Database Servers, page 6-1](#)



PART 3

Configuring the Cisco TelePresence Exchange System

- [Getting Started with Configuration](#)
- [Configuring System Settings](#)
- [Configuring Media Resources](#)
- [Configuring Customers](#)
- [Configuring Endpoints](#)
- [Configuring Call Routing](#)
- [Configuring Collaboration Services](#)
- [Managing Licenses](#)



CHAPTER 7

Getting Started with Configuration

Revised June 29, 2011

Before configuring the Cisco TelePresence Exchange System, there are a number of supporting network systems that you must configure to allow proper operation of the Cisco TelePresence Exchange Solution. The following sections address these network preparations:

- [Prerequisites for Configuring the Cisco TelePresence Exchange System, page 7-1](#)
- [Configuration Task Sequences, page 7-2](#)

Prerequisites for Configuring the Cisco TelePresence Exchange System

Before configuring the Cisco TelePresence Exchange System, ensure that you complete the following prerequisite tasks:

- Install and configure a Cisco Unified Communications Manager.
For additional information, see the [“Configuring Cisco Unified Communications Manager”](#) chapter.
- Install and configure a Cisco router with integrated video response (IVR) capabilities.
For additional information, see the [“Configuring the Cisco Router with IVR”](#) chapter.
- Install and configure a Cisco Application Control Engine (ACE).
For additional information, see the [“Configuring the Cisco Application Control Engine”](#) section on [page 15-3](#).
- Install and configure a Cisco TelePresence Multipoint Switch.
For additional information, see the [“Configuring System Settings”](#) section on [page 16-1](#).
- Install and configure a Cisco TelePresence Manager.
For additional information, see the [“Configuring Cisco TelePresence Manager”](#) chapter.
- Install and configure a Cisco router to function as a SBC.
For additional information, see the [“Configuring Cisco Session Border Controllers”](#) chapter.
- (Optional) Install and configure a Cisco TelePresence MSE 8000 Series system.
For additional information, see the [“Configuring Cisco TelePresence MSE 8000 Series Settings”](#) section on [page 21-2](#).
- Install and configure a Cisco Catalyst Switch that provides Layer 2/ 3 connectivity for the Cisco TelePresence Exchange System and the other Cisco platforms.

Configuration Task Sequences

As dependencies exist between some configuration tasks, Cisco recommends that you do the configuration procedures in the order presented in the following sections:

- [Adding a Service Provider or Region, page 7-2](#)
- [Configuring the Meet-Me Service, page 7-2](#)
- [Configuring the Direct Dial Service, page 7-3](#)
- [Connecting to a Remote Service Provider, page 7-3](#)
- [Configuring Interoperability with Cisco TelePresence MSE 8000 Series, page 7-3](#)

Adding a Service Provider or Region

For the initial configuration of the Cisco TelePresence Exchange System (or when adding a new service provider or region), do the configuration procedures in the following order:

1. Create the service provider.
2. Define a region for the service provider.
3. Configure IVR resources for the region.
4. Configure the CTMS resource.
5. (Optional) Configure the Cisco TelePresence MSE 8000 Series resources that are required for inter-working with H.323 and ISDN standards-based endpoints.
6. Configure the Cisco TelePresence Manager resource, which is only required when the Cisco TelePresence Exchange System hosts endpoints for this organization.
7. Configure the SIP resource, which is required only for the direct dial service.
8. Configure the cluster nodes, which is required for the licensing server and the call details records (CDR) service.
9. Verify that the required product licenses are active.

Configuring the Meet-Me Service

**Note**

You must define a service provider and region before you can configure Meet-Me service components.

To configure the Meet-Me service, do the configuration procedures in the following order:

1. Configure the IVR prompts.
2. Configure the service number.
3. Configure the organizations.
4. Synchronize the provisioned endpoints from Cisco TelePresence Manager and assign an organization to each endpoint.

Configuring the Direct Dial Service

To configure Meet-Me service, do the configuration procedures in the following order:

1. Configure a route for each organization.
2. Configure the endpoints.
3. Configure the adjacencies on the SBC.

Connecting to a Remote Service Provider

**Note**

Direct dial service is not supported for remote service providers.

To configure connectivity to a remote service provider, do the configuration procedures in the following order:

1. Configure a route for the service provider.
2. Configure a dial pattern for the service provider.

Configuring Interoperability with Cisco TelePresence MSE 8000 Series

To configure inter-working functionality, do the configuration procedures in the following order:

1. Configure the Cisco TelePresence MSE 8000 Series supervisor module and optional service modules.
2. Configure the SBC to accommodate the Cisco VCS.



CHAPTER 8

Configuring System Settings

Revised June 29, 2011

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, page 8-1](#)
- [Configuring Cluster Nodes, page 8-2](#)
- [Configuring Time Zones, page 8-4](#)
- [Configuring Users, page 8-4](#)
- [Configuring Database Backups, page 8-7](#)

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.

Live System Ping

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.

Configuring 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. When you remove a cluster node from the network, the system automatically removes the corresponding entry in the administration console. However, you can modify information for a cluster node by using the administration console.



Note

Updates to the administration console can take up to five minutes.

The following sections describe how to modify cluster nodes:

- [Editing Cluster Nodes, page 8-2](#)
- [Deleting Cluster Nodes, page 8-3](#)
- [Cluster Node Fields, page 8-3](#)

Editing Cluster Nodes

Procedure

To edit a Cluster Node, do the following procedure:

-
- Step 1** From the navigation pane, choose **System > Cluster Nodes**.
The Cluster Nodes window is displayed.
- Step 2** In the item table, click the applicable entry.
The node details window is displayed.
- Step 3** From the toolbar, click **Edit this Cluster Node**.
The Edit Node window is displayed. Fields contain the currently-configured values.
- Step 4** Modify field entries as required.
Fields are described in [Table 8-1](#).
- Step 5** To save your changes, click **Save**.
-

Deleting Cluster Nodes

Procedure

To delete a cluster node, do the following procedure:

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

The Cluster Nodes window is displayed.

Step 2 Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- a. In the item table, check the check box next to the entry that you want to delete. You can delete multiple cluster nodes 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.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that opens to confirm the deletion, click **OK**.



Tip

If you prefer to view the details of a cluster node prior to deleting it, in the Cluster Nodes window, you can click the applicable **Cluster Node** to go to the Cluster Node page. After verifying that you have chosen the correct cluster node to delete, click **Delete This Cluster Node**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Cluster Node Fields

Table 8-1 Cluster Node Field Descriptions

Field	Description
Node Name	Node name of the 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	Drop-down list of clusters. Currently, Default Cluster is the only choice.
Node Type	Drop-down list of node types. For the licensing server, choose ENGINE. For the CDR collection service, choose ADMIN. For the database server, choose 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 define a time zone to allow configuration of the time of day within the administration console such as setting the starting time for a meeting.

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

System administrators can create new users and modify user settings such as name, user ID, email, and password.

The Cisco TelePresence Exchange System administration console supports the following user roles:

- **System**—System administrators have the authority to configure or modify all settings that are associated with the Cisco TelePresence Exchange System. The system administrator can create new users and assign roles to all users.
- **Admin**—Administrators have the authority to configure or modify all settings that are associated with the Cisco TelePresence Exchange System. Admin users can create API users.
- **Provisioning**—(available only in Cisco TelePresence Exchange System Release 1.0(3) and later)
Provisioning users can log in to the administrative console, and can modify data on the Customers and Endpoint Management pages only. For all other pages in the system, the provisioning user has read-only privileges, and the add, edit, and delete buttons are hidden. Provisioning users can be created by system administrators with the System user role.
- **Read only**—(available only in Cisco TelePresence Exchange System Release 1.0(3) and later)
Read-only users can log in to the administrative console to view pages, but all add, edit, and delete buttons are hidden from them. Read-only users can be created by system administrators with the System user role.
- **API**—The API role allows billing and operational systems to access the Cisco TelePresence Exchange System API. Systems that access the API cannot access the administration console. For additional information about the API, see 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.

The following sections describe how to configure users:

- [Adding Users](#), page 8-5
- [Editing User Settings](#), page 8-5
- [Deleting Users](#), page 8-6
- [User Fields](#), page 8-7

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 8-2](#) 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.
- 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 8-2](#).

- 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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- a. 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.
- b. Click **Delete**.
- c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.



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 8-2 **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. Note You can also reach the Systems > Users window by clicking the username link in the banner pane. For more details, see the “ Banner Pane ” section on page 2-2.
Verify Password	Password entered again for verification.
Role	Drop-down list. Sets the role of the user: <ul style="list-style-type: none"> • System—System Administrator • Admin—Administrator • Provisioning (<i>available only in Cisco TelePresence Exchange System Release 1.0(3) and later</i>)—A user with access only to the Customers and Endpoint Management pages • Read Only (<i>available only in Cisco TelePresence Exchange System Release 1.0(3) and later</i>)—A user with read-only access • API—A user with access to the Cisco TelePresence Exchange System API
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 8-4.

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.



Note

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 23-1.



Note

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:
- Enter either the server name (if DNS is in use) or the IP address.
 - Enter the directory path to the server.
 - Enter the username and password for the server.
 - Choose the transfer protocol from the drop-down list.
 - 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**.
-



CHAPTER 9

Configuring Media Resources

Revised June 29, 2011

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, page 9-1](#)
- [Configuring SIP Resources, page 9-4](#)
- [About Media Resources for Large Meetings, page 9-6](#)
- [Configuring CTMS Resources, page 9-6](#)
- [Configuring TPS Resources, page 9-10](#)
- [Configuring MSE 8510 Resources, page 9-13](#)

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, page 9-1](#)
- [Editing IVR Resources, page 9-2](#)
- [Deleting IVR Resources, page 9-2](#)
- [IVR Resource Fields, page 9-3](#)

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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
Cisco TelePresence Exchange System Release 1.0(3)
- a. 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.
 - b. Click **Delete**.

- c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.



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 10-4.
Operational State	(Optional) Drop-down list of operational states for the Cisco router. Choose OFFLINE . The system automatically updates the operational state when the IVR resource becomes available. See the “Media Resource Operational States” section on page 2-4.
Max Capacity	You can ignore this field. The default value is 255.
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 UDP or TCP . This value must match the configuration on the IVR resource.

Configuring SIP Resources

The service provider SBC 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, page 9-4](#)
- [Editing SIP Resources, page 9-4](#)
- [Deleting SIP Resources, page 9-5](#)
- [SIP Resource Fields, page 9-6](#)

Adding SIP Resources

Before You Begin

Install and configure the Cisco SBC. For additional information, 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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
- Cisco TelePresence Exchange System Release 1.0(3)**
- 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.
 - Click **Delete**.
 - In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.
- Cisco TelePresence Exchange System Release 1.0(2) and earlier**
- In the item table, check the check box next to the entry you want to delete.
 - From the drop-down list that appears, choose **Delete**.
 - Click **Go**.
 - In the panel that is displayed to confirm the deletion, click **OK**.



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 10-4.
Maintenance	Check box. Check the check box to set the Cisco TelePresence Multipoint Switch 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 UDP or TCP . This value must match the configuration on the SBC.

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 eight or more endpoints and are scheduled exclusively on media units that are reserved for large meetings.
- Regular meetings (meetings with seven or fewer endpoints) 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 need to configure information about the Cisco TelePresence Multipoint Switch cluster that is associated with this Cisco TelePresence Exchange System.

The following sections describe how to configure CTMS resources:

- [Adding CTMS Resources, page 9-7](#)
- [Editing CTMS Resources, page 9-7](#)
- [Deleting CTMS Resources, page 9-8](#)
- [CTMS Resource Fields, page 9-8](#)

Adding CTMS Resources

Before You Begin

Install and configure the Cisco TelePresence Multipoint Switch. For additional information, see the “[Configuring the Cisco TelePresence Multipoint Switch](#)” chapter.

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

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

Before You Begin

Delete any completed meetings that used this CTMS resource.

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 Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- a. 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.
- b. Click **Delete**.
- c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.



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.

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.

Table 9-3 CTMS Resource Field Descriptions (continued)

Field	Description
Region	Drop-down list of the available regions. See the “Adding Regions” section on page 10-4.
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 Meet-Me meeting on this Cisco TelePresence Multipoint Switch. The range of this field is 1 to 48. 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.
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 which specifies the transport protocol between the Cisco TelePresence Exchange System and the Cisco TelePresence Multipoint Switch. Choose either UDP or TCP . This value must match the configuration on the Cisco TelePresence Multipoint Switch.
Test CTMS	Check box. When you check the Test field check box, the Cisco TelePresence Multipoint Switch is available for test meetings only. A test system is not available for scheduling regular meetings.
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 eight or more endpoints. For additional information about the implications of large meetings, see the “About Media Resources for Large Meetings” section on page 9-6.
Vendor Config	A range of static meeting identifiers and interop meeting identifiers that are defined on this Cisco TelePresence Multipoint Switch. The Cisco TelePresence Exchange System uses this information to ensure that requests to join statically-defined meetings are fulfilled by using the Cisco TelePresence Multipoint Switch on which the static meeting is defined. For the Min Interop Meeting ID field, you must enter a value of 1. For the Max Interop Meeting ID field, you must enter a value of 2. For additional information about static meetings, see the “Creating Static Meetings” section on page 16-9.

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.

The following sections describe how to configure TPS resources:

- [Adding TPS Resources, page 9-10](#)
- [Editing TPS Resources, page 9-10](#)
- [Deleting TPS Resources, page 9-11](#)
- [TPS Resource Fields, page 9-11](#)

Adding TPS Resources

Before You Begin

Install and configure the Cisco TelePresence Server MSE 8710. For additional information, see the [“Configuring Cisco TelePresence Server MSE 8710 Settings” section on page 21-3](#).

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

To delete 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 Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- a. 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.
- b. Click **Delete**.
- c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.



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.

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.

Table 9-4 TPS Resource Field Descriptions (continued)

Field	Description
Region	Drop-down list of the available regions. See the “Adding Regions” section on page 10-4.
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 Meet-Me meeting on this Cisco TelePresence Server MSE 8710. The range of this field is 1 to 48. The default value is 48 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. Choose UDP or TCP from the drop-down list to specify the transport protocol between the Cisco TelePresence Exchange System and the Cisco TelePresence Server MSE 8710. The selected transport protocol must match the protocol setting on the Cisco TelePresence Server MSE 8710.
Test TPS	Check box. Check the check box to reserve the Cisco TelePresence Server MSE 8710 for test meetings only. When serving as a test system, the resource is not available as a resource for scheduling regular meetings.
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 eight or more endpoints. For additional information about the implications of large meetings, see the “About Media Resources for Large Meetings” section on page 9-6.
Vendor Config	Defines a range of permanent meeting identifiers and E.164 numbers for the Cisco TelePresence Server MSE 8710. The Cisco TelePresence Exchange System uses this information to ensure that requests to join statically-defined meetings are fulfilled by using the Cisco TelePresence MCU MSE 8510 on which the static meeting is defined. Cisco recommends that you use a four-digit number range for the Cisco MSE 8710 and 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. For additional information about static meetings, see the “Creating Static Meetings” section on page 16-9.

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, page 9-13](#)
- [Editing MSE 8510 Resources, page 9-13](#)
- [Deleting MSE 8510 Resources, page 9-14](#)
- [MSE 8510 Resource Fields, page 9-14](#)

Adding MSE 8510 Resources

Before You Begin

Install and configure the Cisco TelePresence MCU MSE 8510. For additional information, see the [“Configuring Cisco TelePresence MSE 8000 Series”](#) chapter.

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

To delete a 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 Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- a. 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.
- b. Click **Delete**.
- c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.



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.

MSE 8510 Resource Fields

Table 9-5 MSE 8510 Resource 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.

Table 9-5 *MSE 8510 Resource Field Descriptions (continued)*

Field	Description
Region	Drop-down list of the available regions. See the “Adding Regions” section on page 10-4.
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 Meet-Me meeting on this Cisco TelePresence MCU MSE 8510. The range of this field is 1 to 48. The default value is 48 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 UDP or TCP . This value must match the configuration on the Cisco TelePresence MCU MSE 8510.
Test MSE 8510	Check box. When you check the Test field check box, you reserve the Cisco TelePresence MCU MSE 8510 for test meetings only and the system is not available as a resource for scheduling regular meetings.
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 eight or more endpoints. For additional information about the implications of large meetings, see the “About Media Resources for Large Meetings” section on page 9-6.
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 ensure that requests to join permanent meetings are fulfilled by using the MCU on which the permanent meeting is defined. For additional information about static and permanent meetings, see the “Creating Static Meetings” section on page 16-9.



CHAPTER 10

Configuring Customers

Revised June 29, 2011

The following sections describe how to configure service providers and their customer settings:

- [Configuring Service Providers, page 10-1](#)
- [Configuring Regions, page 10-4](#)
- [Configuring Organizations, page 10-6](#)

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, page 10-1](#)
- [Editing Service Providers, page 10-2](#)
- [Deleting Service Providers, page 10-2](#)
- [Service Provider Fields, page 10-3](#)

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 delete 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 regions. Other items (such as media resources) might indirectly depend on a specific service provider because they are associated with a region.



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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
Cisco TelePresence Exchange System Release 1.0(3)
- 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.

- b. Click **Delete**.
- c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.



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 .

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 Systems, 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, page 10-4](#)
- [Editing Regions, page 10-4](#)
- [Deleting Regions, page 10-5](#)
- [Region Fields, page 10-6](#)

Adding Regions

Before You Begin

Configure the service provider that you want to associate with the region.

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 must delete all of the configuration items (such as media resources) that are dependencies of this region. The media resources of this region can be reassigned to another region.



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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
- Cisco TelePresence Exchange System Release 1.0(3)**
- 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.
 - Click **Delete**.
 - In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.
- Cisco TelePresence Exchange System Release 1.0(2) and earlier**
- In the item table, check the check box next to the entry you want to delete.
 - From the drop-down list that appears, choose **Delete**.
 - Click **Go**.
 - In the panel that is displayed to confirm the deletion, click **OK**.



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.
Service Provider	Drop-down list of the available service providers. Choose the service provider to associate it with this region. See the “Adding Service Providers” section on page 10-1.

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](#), page 10-6
- [Editing Organizations](#), page 10-7
- [Deleting Organizations](#), page 10-7
- [Organization Fields](#), page 10-8

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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
- Cisco TelePresence Exchange System Release 1.0(3)**
- 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.
 - Click **Delete**.
 - In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.
- Cisco TelePresence Exchange System Release 1.0(2) and earlier**
- In the item table, check the check box next to the entry you want to delete.
 - From the drop-down list that appears, choose **Delete**.

- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.

**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.

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.
Direct Dial Enabled	Check the check box to enable the organization to use the direct dial feature.
Minimize Capacity	<i>(Applicable to Cisco TelePresence Exchange System Release 1.0(3) and later only)</i> 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.
SIP Routes	When you enable direct-dial, you must add at least one route to the SBC resource. You can add multiple routes, and order by priority, to accommodate SBC fail over. (This field is displayed only when you check the Direct Dial Enabled check box).



CHAPTER 11

Configuring Endpoints

Revised June 29, 2011

The following sections describe how to configure endpoints:

- [Configuring Endpoints, page 11-1](#)
- [Configuring Media Profiles, page 11-4](#)
- [Configuring CTS Manager Resources, page 11-7](#)

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. Meet-Me and Direct Dial calls are placed on provisioned endpoints.
- **Unprovisioned endpoints**—Endpoints for which none of the configuration details are known by the administrator except the name of the organization that schedules meetings for the endpoint. Through the administration console you can reserve bandwidth for unprovisioned endpoints on the service provider network. This allows the endpoint to connect with other known endpoints within the network that are scheduled for the same meeting. This capability is useful for intercompany meetings.
- **Remote endpoints**—Endpoints for which no configuration details are known. Remote endpoints are endpoints that join the meeting from another service provider network. Configuring a remote endpoint on the Cisco TelePresence Exchange System reserves capacity for the endpoint on the service provider network on which it is resident. The Cisco TelePresence Exchange System automatically determines and reserves the capacity to support these interprovider meetings.

The following sections describe how to configure endpoints:

- [Adding Endpoints, page 11-2](#)
- [Editing Endpoints, page 11-2](#)
- [Deleting Endpoints, page 11-2](#)
- [Endpoints Fields, page 11-3.](#)

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 is displayed.
 - 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**.
-

Deleting Endpoints

Procedure

To delete an endpoint, do the following procedure:

-
- Step 1** From the navigation pane, choose **Endpoint Management > Endpoints**.
The Endpoint window is displayed.
 - Step 2** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- 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.



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

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, click the entry that you want to delete.
- b. Details for the endpoint display.
- c. From the toolbar, click **Delete This Endpoint**.
- d. To confirm deletion of the endpoint, click **OK** in the panel that is displayed.

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. Enter the phone number for the endpoint. Note There is no need to note a country code in the number.
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. Note OBTP support is available only for TIP-based Cisco TelePresence System endpoints.

Table 11-1 Endpoint Field Descriptions (continued)

Field	Description
CTS-MAN	<p>(Optional) Is displayed when you check the Support OBTP check box.</p> <p>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.</p> <p>Note For more details on the Unified CM settings set on the Cisco TelePresence Manager, see the “Configuring Cisco Unified Communications Manager” chapter.</p> <p>This field is required only for endpoints that support OBTP.</p>
Hosted Room	<p>(Optional) Is displayed when you check the Support OBTP check box.</p> <p>Drop-down list of hosted rooms available on the Cisco TelePresence Manager. Choose the room that corresponds to this endpoint.</p> <p>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.</p>

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. Pre-defined media profiles exist for Cisco endpoints. 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, page 11-4](#)
- [Editing Media Profiles, page 11-5](#)
- [Deleting Media Profiles, page 11-5](#)
- [Media Profile Fields, page 11-6](#)

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

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

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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
- Cisco TelePresence Exchange System Release 1.0(3)**
- 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.
 - Click **Delete**.
 - In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.
- Cisco TelePresence Exchange System Release 1.0(2) and earlier**
- In the item table, check the check box next to the entry you want to delete.
 - From the drop-down list that appears, choose **Delete**.
 - Click **Go**.
 - In the panel that is displayed to confirm the deletion, click **OK**.

**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 .
Video Bandwidth	(Optional) Numeric value in megabits per second (Mbit/s). When set, specifies the maximum video bandwidth allowed for the endpoint type. When no value is set for this field, there is no maximum. Note Cisco recommends that you leave this field blank unless network conditions require an adjustment.
Audio Bandwidth	(Optional) Numeric value in megabits per second (Mbit/s). Sets the maximum audio bandwidth available for the endpoint type. When no value is set for this field, there is no maximum. Note Cisco recommends that you leave this field blank unless network conditions require an adjustment.
Number of Screens	Numeric value. Enter the number of screens (segments) that this endpoint type provides.
Protocol	Drop down list. Choose the signaling protocol required for this endpoint type. The choices include ISDN, H323, and SIP.
Participant Type	Drop down list. Choose the value that corresponds to this endpoint type. The choices include: <ul style="list-style-type: none"> T3—Cisco TelePresence three-screen endpoint. CTS—Cisco TelePresence TIP-based endpoint. (When you choose this option, it attempts to detect the number of screens automatically). CTS1—Cisco TelePresence TIP-based one-screen endpoint. CTS3—Cisco TelePresence TIP-based three-screen endpoint.

Table 11-2 Media Profile Field Descriptions (continued)

Field	Description
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.

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, page 11-7](#)
- [Editing CTS Manager Resources, page 11-8](#)
- [Deleting CTS Manager Resources, page 11-8](#)
- [CTS Manager Fields, page 11-9](#)

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** (Optional) 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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- a. 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.
- b. Click **Delete**.
- c. 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.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, click the entry that you want to delete.
- b. The CTS-MAN Resource Details window is displayed.
- c. In the toolbar, click **Delete This CTS-MAN Resource**.

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 .
Host	The IP address (or hostname, if DNS is enabled) 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

Revised June 29, 2011

The following sections describe how to configure call routing by using the administrative console:

- [Configuring Routes, page 12-1](#)
- [Configuring Dial Patterns, page 12-4](#)
- [Configuring Remote Service Providers, page 12-6](#)
- [Viewing Call Detail Records, page 12-9](#)

Configuring Routes

On the Cisco TelePresence Exchange System, a route is a reference to an adjacency on a Cisco Session Border Controller (SBC). Each adjacency on the SBC is assigned a unique tag. The tag value is included in SIP messages between the SBC and Cisco TelePresence Exchange System, which simplifies routing.

For example, the SBC uses an adjacency for each hosted organization. The adjacency is configured with a unique tag. The same tag value is configured in the Cisco TelePresence Exchange System route for that organization. Therefore, the outgoing route on the SBC is found by matching the tag value.

The following sections describe how to configure routes:

- [Adding Routes, page 12-1](#)
- [Editing Routes, page 12-2](#)
- [Deleting Routes, page 12-2](#)
- [Route Fields, page 12-3](#)

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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
- Cisco TelePresence Exchange System Release 1.0(3)**
- 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.
 - Click **Delete**.
 - In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.
- Cisco TelePresence Exchange System Release 1.0(2) and earlier**
- In the item table, check the check box next to the entry you want to delete.
 - From the drop-down list that appears, choose **Delete**.
 - Click **Go**.

- d. In the panel that is displayed to confirm the deletion, click **OK**.

**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. If the route is for direct-dial or help desk calls, choose BOTH. If the route is for a remote service provider, you can specify separate routes for incoming and outgoing calls.

Table 12-1 Route Field Descriptions (continued)

Field	Description
Endpoint Type	<p>Drop-down list. Choose one of the following values:</p> <ul style="list-style-type: none"> • 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. <p> 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.</p>
Active	Check box. Check this check box to activate the route.

Configuring Dial Patterns

A dial pattern is a digit pattern that matches the rule that you configure for the system. You can specify the rule as a regular expression or as a set of digits to match exactly.

You can also match the domain (which are the characters that follow the @ symbol in the SIP URI).

The following sections describe how to configure dial patterns:

- [Adding Dial Patterns, page 12-4](#)
- [Editing Dial Patterns, page 12-5](#)
- [Deleting Dial Patterns, page 12-5](#)
- [Dial Patterns Fields, page 12-6](#)

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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
- Cisco TelePresence Exchange System Release 1.0(3)**
- 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.
 - Click **Delete**.
 - In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.
- Cisco TelePresence Exchange System Release 1.0(2) and earlier**
- In the item table, check the check box next to the entry you want to delete.
 - From the drop-down list that appears, choose **Delete**.
 - Click **Go**.
 - In the panel that is displayed to confirm the deletion, click **OK**.

**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	The definition of the pattern. The format of the pattern field depends on the pattern type.
Pattern Type	Drop-down list. The pattern type specifies how the Cisco TelePresence Exchange System will use the contents of the pattern field to match the dial pattern. The available pattern type is Number, which matches the exact number that is entered in the pattern. •

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 12-7](#)
- [Editing Remote Service Providers, page 12-7](#)
- [Deleting Remote Service Providers, page 12-7](#)
- [Remote Service Provider Fields, page 12-8](#)

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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- a. 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.
- b. Click **Delete**.
- c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.



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 .
Description	Text string describing the remote service provider. See the “Common Field Properties” section on page 2-4 .

Table 12-3 Remote Service Provider Field Descriptions (continued)

Field	Description
Dial Patterns	<p>Button and drop-down list.</p> <p>Click Add A Dial Pattern to display a drop-down list.</p> <p>To associate a dial pattern with the remote service provider, choose a dial pattern from the drop-down list.</p> <p>You can add multiple dial patterns by repeating the above procedure.</p> <p>For information about dial patterns, see the “Adding Dial Patterns” section on page 12-4.</p>
SIP Routes	<p>Button and drop-down list.</p> <p>Click Add A Route to display a drop-down list.</p> <p>To associate a SIP route with the remote service provider, choose a route from the drop-down list.</p> <p>Note SBCs manage call routing between the Cisco TelePresence Exchange System and remote service providers.</p> <p>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.</p> <p>For information about routes, see the “Adding Routes” section on page 12-1.</p>

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 system saves up to 30 days of CDR information and deletes any records older than 30 days on a daily basis.

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 12-9](#)
- [Exporting a CDR File, page 12-10](#)

For instructions on viewing intra-company call detail records, see the [“Viewing Intra-Company CDRs” section on page 12-10](#).

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.

- 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.

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 pull the CDRs from Cisco Unified Communications Manager and to generate them locally as if the calls had been processed by the Cisco TelePresence Exchange System itself.



Note

- The collected CDRs are stored on the Cisco TelePresence Exchange System with all the other CDRs, with the cdrSource set to INTRACOMPANY_DIRECTDIAL.

- 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.

See the following “[Configuring Unified CM to Enable Intra-Company CDRs](#)” section for detailed instructions.

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** 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 June 29, 2011

The following sections describe how to configure collaboration services:

- [Configuring Service Numbers, page 13-1](#)
- [Configuring IVR Prompts, page 13-3](#)
- [Scheduling Meetings, page 13-6](#)
- [Scheduling Standing Meetings, page 13-11](#)

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, page 13-1](#)
- [Editing Service Numbers, page 13-2](#)
- [Deleting Service Numbers, page 13-2](#)
- [Service Number Fields, page 13-3](#)

Adding Service Numbers

Before You Begin

Configure the service provider and IVR resources 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** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
- Cisco TelePresence Exchange System Release 1.0(3)**
- a. 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.
 - b. Click **Delete**.
 - c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.
- Cisco TelePresence Exchange System Release 1.0(2) and earlier**
- a. In the item table, check the check box next to the entry you want to delete.
 - b. From the drop-down list that appears, choose **Delete**.
 - c. Click **Go**.
 - d. In the panel that is displayed to confirm the deletion, click **OK**.

**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).
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 13-4 .

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 different organizations or for different languages or they can employ the default Cisco IVR prompts.

The following sections describe how to configure service numbers:

- [Adding IVR Prompts, page 13-4](#)
- [Editing IVR Prompts, page 13-4](#)
- [Deleting IVR Prompts, page 13-5](#)
- [IVR Prompt Fields, page 13-5](#)

Adding IVR Prompts

Before You Begin

Install and configure the Cisco router.

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 13-2](#) 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 13-2](#) 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 Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- a. 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.
- b. Click **Delete**.
- c. In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.



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 13-2 *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 .
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 13-2 *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	<i>Applicable only to Cisco TelePresence Exchange System Release 1.0(3) and later.</i> Text string indicating the location of the voice file for the No Conference Resource Available 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 13-6](#)
- [Scheduling Meetings, page 13-7](#)
- [Schedule Meeting Fields, page 13-8](#)

For information on meeting diagnostics, see the “[Meeting Diagnostics](#)” chapter.

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.

- Step 2** For instructions on viewing additional information about scheduled and complete meetings, see the applicable section:
- [Viewing Meeting Diagnostics \(Cisco TelePresence Exchange System Release 1.0\(3\) and Later Only\)](#), page 24-2
 - [Viewing Meeting Diagnostics \(Cisco TelePresence Exchange System Release 1.0\(2\) and Earlier Only\)](#), page 24-5
-

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.
[Table 13-3](#) describes the meeting fields.
- Step 4** To save your changes, click **Schedule**.
-

Schedule Meeting Fields

Table 13-3 Schedule Meeting Field Descriptions

Field	Description
Meeting Type	<p>Radio buttons provide a choice of MeetMe, Remote, or Two Party Direct.</p> <ul style="list-style-type: none"> • 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. • 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). <p>Note Beginning with Cisco TelePresence Exchange System release 1.0(3), 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.</p>
Test	<p>Check box.</p> <p>Check the Test check box to allow test meetings to be run.</p> <p>For information about configuring test units, see the “Configuring CTMS Resources” section on page 9-6.</p> <p>Test meetings do not generate billing records.</p> <p>Note Test meetings are allocated exclusively on Cisco TelePresence Multipoint Switch test units and are an option only for Meet-Me meetings.</p> <p>Note The Test check box is displayed only when scheduling a Meet-Me meeting.</p> <p>Note When you check this check box, the only resources shown in the Resource drop-down list are those that you have designated for test purposes. If the Resource drop-down list is empty, you must first add a test resource, making sure to check the Test check box on the Resource page to designate it for test purposes.</p>
Service Provider	Drop-down list of service providers. Choose the service provider that will host this meeting.
Subject	Text description of the 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 13-3 Schedule Meeting Field Descriptions (continued)

Field	Description
Conference ID	Text field. Enter a unique, eight-digit conference ID for users to dial to reach this meeting. Note This field is displayed only on the Remote Meetings configuration window.
Access Number	Number that the participant must call to reach the meeting. Note This field is displayed only on the Remote Meetings configuration window.
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.
Duration	Duration of the meeting in minutes.
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. Note This field is displayed only when scheduling a Meet-Me meeting.
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. Note This field is displayed only when scheduling a Meet-Me meeting.
Request Specific Resource	<i>Applicable only to Cisco TelePresence Exchange System Release 1.0(3) and later.</i> Check box. Check the check box if you want the system to display a drop-down list of available resources. When this check box is checked, you must select a resource from the Resource list. Note The Request Specific Resource check box is available only when a Region is selected.
Resource	<i>Applicable only to Cisco TelePresence Exchange System Release 1.0(3) and later.</i> A drop-down list of available resources, filtered by region. When the Request Specific Resource check box is checked, you must select a resource from this list. When you specify a resource in this field, then only that resource can be used for this meeting. If the selected resource is offline at the time of the meeting, the meeting will fail. Note The Resource list is available only when the Request Specific Resource check box is checked. Note When you check the Test check box, the only resources shown in this drop-down list will be resources that are designated for test purposes.

Table 13-3 Schedule Meeting Field Descriptions (continued)

Field	Description
Additional Bridge Capabilities	<p>Sets the required bridge capabilities for unprovisioned endpoints in the meeting. You can select more than one bridge option.</p> <p>Note For provisioned endpoints, the system automatically detects the bridging capabilities.</p> <ul style="list-style-type: none"> • TelePresence Endpoints—Select this option if a TIP-based Cisco TelePresence System is in the meeting. • Single-screen Interop Endpoints—Select this option if any single-screen, standards-based (H323, ISDN) endpoint is in the meeting. • Multi-screen Interop Endpoints—Select this option if a three-screen Cisco TelePresence T3 is in the meeting. <p>Note This field is displayed only when scheduling a Meet-Me meeting.</p>
Additional Capacity	<p>Number of additional ports/segments that the system needs to reserve for the meeting. The value must be multiples of 4.</p> <p>For planning purposes, each three-screen endpoint requires 4 ports, and each single-screen endpoint requires 2 ports.</p> <p>Note This field is displayed only when scheduling a Meet-Me meeting.</p>
Provisioned Endpoints	<p>Provisioned meetings are Meet-Me or Two Party Direct calls that you provision on the Cisco TelePresence Exchange System.</p> <p>The system is aware of all details about the meeting (such as number of screens, and organization). The provisioned meeting might or might not have a connection to a Cisco TelePresence Manager for OBTP support.</p> <p>Click Add Provisioned Endpoints to display a drop-down list of provisioned endpoints, and choose an endpoint to include in this meeting.</p> <p>Ports is the number of ports/segments that the endpoint requires. By default, the system reserves four ports/segments of capacity for each provisioned endpoint.</p> <p>To add an additional endpoint, click Add Provisioned Endpoints again.</p> <p>Note The Remote Endpoints button is not an option for Remote meetings.</p>

Table 13-3 Schedule Meeting Field Descriptions (continued)

Field	Description
Unprovisioned Endpoints	<p>Unprovisioned meetings reserve ports for an unknown endpoint for a specific organization.</p> <p>Click Add Unprovisioned Endpoints to display a drop-down list of organization names, and choose an organization to include in this meeting.</p> <p>Ports is the number of segments that the endpoint requires. The default value is zero.</p> <p>To allow the endpoint to receive guest dial-out calls, check the Guest Dial Out check box.</p> <p>Enter the number that the system must dial to reach the guest endpoint.</p> <p>From the Endpoint Protocol drop-down list, choose the signaling protocol for the endpoint (ISDN, SIP, H323).</p> <p>To add an additional endpoint, click Add Unprovisioned Endpoints again.</p> <p>Note The Unprovisioned Endpoints button is not an option for Two-Party Direct meetings.</p>
Remote Endpoints	<p>Reserves capacity for a remote endpoint for an inter-service provider participant. No additional data is visible or configurable for this type of endpoint.</p> <p>To reserve capacity for a remote endpoint, click Add Remote Endpoints. A Remote Endpoint entry is displayed on the window.</p> <p>No additional configuration is possible.</p> <p>Note The Add Remote Endpoints button is displayed only when you select the Meet-Me radio button.</p>

Scheduling Standing Meetings

Scheduling a standing meeting allows you to verify the operation of the system or to establish a demonstration meeting. For example, you can provision an endpoint and then call in to the standing meeting to verify connectivity to the Cisco TelePresence Exchange System without involving other endpoints or participants.

A standing meeting is a permanent meeting that you configure on a Cisco TelePresence Multipoint Switch and that you name as a test resource. You cannot configure a standing meeting in a region that does not have a Cisco TelePresence Multipoint Switch test resource.

The following sections describe how to add, change, and delete standing meetings:

- [Adding Standing Meetings, page 13-12](#)
- [Editing Standing Meetings, page 13-12](#)
- [Deleting Standing Meetings, page 13-13](#)
- [Standing Meeting Fields, page 13-13](#)

Adding Standing Meetings

**Note**

On the Cisco TelePresence MSE 8000 Series, standing meetings are known as permanent meetings. On the Cisco TelePresence Multipoint Switch, standing meetings are known as static meetings.

Before You Begin

Configure the service provider and region.

Procedure

To add a new standing meeting, do the following procedure:

-
- Step 1** From the navigation pane, choose **Collaboration Services > Standing Meetings**.
The Standing Meetings window is displayed.
 - Step 2** Click **Add A New Standing Meeting**.
 - Step 3** Enter the settings as indicated in [Table 13-4](#) to configure the standing meeting.
 - Step 4** To save your changes, click **Save**.
-

Editing Standing Meetings

Procedure

To edit a standing meeting, do the following procedure:

-
- Step 1** From the navigation pane, choose **Collaboration Services > Standing Meetings**.
The Standing Meetings window is displayed.
 - Step 2** In the item table, click the applicable entry.
The Standing Meeting Details window is displayed.
 - Step 3** From the toolbar, click **Edit This Standing Meeting**.
The Edit Standing Meeting window is displayed. Fields contain the currently-configured values.
 - Step 4** Modify field entries as required.
Fields are described in [Table 13-4](#).
 - Step 5** To save your changes, click **Save**.
The Standing Meeting Details window is displayed. Modified fields display the new values.
-

Deleting Standing Meetings

Procedure

To delete a standing meeting, do the following procedure:

-
- Step 1** From the navigation pane, choose **Collaboration Services > Standing Meetings**.
The Standing Meetings window is displayed.
- Step 2** Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.
- Cisco TelePresence Exchange System Release 1.0(3)**
- In the item table, check the check box next to the entry that you want to delete. You can delete multiple standing meetings at one time by checking the check box next to each entry that you want to delete.
 - Click **Delete**.
 - In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.
- Cisco TelePresence Exchange System Release 1.0(2) and earlier**
- In the item table, check the check box next to the entry you want to delete.
 - From the drop-down list that appears, choose **Delete**.
 - Click **Go**.
 - In the panel that is displayed to confirm the deletion, click **OK**.



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

Standing Meeting Fields

Table 13-4 Standing Meeting Field Descriptions

Field	Description
Name	Text string that identifies the standing meeting. See the “Common Field Properties” section on page 2-4 .
Description	Text string describing this meeting. 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 10-4 .
Conference ID	Text field. Enter a unique, eight-digit conference ID for users to dial to reach this meeting.

Table 13-4 *Standing Meeting Field Descriptions (continued)*

Field	Description
Capacity	Numeric field. The units are ports and segments. For each three-screen endpoint, plan for four ports (segments), and for each single-screen endpoint, plan for two ports (segments).
Schedule Time	The resources for the meeting are re-established every 24 hours at the scheduled time. The standing meeting is unavailable for approximately one minute during this operation. Text field to specify the hour. Drop-down list to select AM or PM. Drop-down list to choose the time zone.
Active	Check box. Check the Active check box to activate the standing meeting.



CHAPTER 14

Managing Licenses

Revised June 29, 2011

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, page 14-1](#)
- [Uploading Licenses, page 14-2](#)

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 **Choose File**.
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

- [Configuring the Cisco Application Control Engine](#)
- [Configuring the Cisco TelePresence Multipoint Switch](#)
- [Configuring the Cisco Router with IVR](#)
- [Configuring Cisco Unified Communications Manager](#)
- [Configuring Cisco TelePresence Manager](#)
- [Configuring Cisco Session Border Controllers](#)
- [Configuring Cisco TelePresence MSE 8000 Series](#)
- [Configuring Internet Group Management Protocol for Multicast Support](#)



CHAPTER 15

Configuring the Cisco Application Control Engine

Revised June 29, 2011

The following sections describe how to configure the Cisco Application Control Engine:

- [About the Cisco Application Control Engine, page 15-1](#)
- [Configuring the Cisco Application Control Engine, page 15-3](#)

About the Cisco Application Control Engine

This section describes the Cisco Application Control Engine (ACE) and includes the following topics:

- [ACE Overview, page 15-1](#)
- [ACE Topology, page 15-1](#)
- [Configuration Overview, page 15-2](#)

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 15-3](#).

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/vA3_1_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/vA3_1_0/configuration/admin/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:

- [Configuring the Hostname, page 15-4](#)
- [Configuring Interfaces, page 15-5](#)
- [Configuring Real Servers, page 15-7](#)
- [Configuring Access Control Lists, page 15-7](#)
- [Configuring Health Probes, page 15-8](#)
- [Creating Server Farms, page 15-10](#)
- [Configuring Session Persistence, page 15-11](#)
- [Configuring Class Maps, page 15-13](#)

- [Configuring Policy Maps, page 15-16](#)
- [Configuring VLAN Interfaces, page 15-19](#)
- [Configuring Miscellaneous Parameters, page 15-22](#)
- [Configuring ACE Logging Options, page 15-24](#)



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 .
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).
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.

	Command	Purpose
Step 14	ACE_1/Admin(config-if) # switchport access vlan <i>vlan_ID</i>	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 <i>name</i>	Enters real server configuration mode for the specified real server.
Step 2	ACE_1/Admin(config-rserver-host)# ip address <i>ip_address</i>	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 <i>probe_name</i>	Creates an HTTP probe with the specified name and enters HTTP probe configuration mode.
Step 2	ACE_1/Admin(config-probe-http)# port <i>port-number</i>	Configures the destination port number to use for the probe.
Step 3	ACE_1/Admin(config-probe-http)# interval <i>seconds</i>	Configures the time interval between probes (in seconds). The default value is 15 seconds.
Step 4	ACE_1/Admin(config-probe-http)# faildetect <i>retry-count</i>	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 <i>seconds</i>	Configures the time interval (in seconds) between sending probes to a failed server.
Step 6	ACE_1/Admin(config-probe-http)# request method <i>get</i> [<i>url</i> <i>url_string</i>]	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.
Step 7	ACE_1/Admin(config-probe-http)# expect status <i>min_number</i> <i>max_number</i>	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 <i>min_value</i> and <i>max_value</i> .
Step 8	ACE_1/Admin(config-probe-http)# open <i>timeout</i>	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
/?wicket:bookmarkablePage=:com.cisco.txbu.ctx.markup.pages.LoginPage
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 /MeetMeIVR/MeetingID?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} <i>name</i>	Enter the type of SIP probe (UDP or TCP) and the name of the probe.
Step 2	ACE_1/Admin(config-probe-sip)# interval <i>seconds</i>	Configures the time interval between probes (in seconds). The default value is 15 seconds.
Step 3	ACE_1/Admin(config-probe-sip)# faildetect <i>retry-count</i>	Configures the number of consecutive failed probes before the server state is marked as failed. The default value is 2.
Step 4	ACE_1/Admin(config-probe-sip)# passdetect interval <i>seconds</i>	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 <i>number</i>	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 <i>min_number</i> <i>max_number</i>	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 <i>timeout</i>	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.
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, page 15-11](#)
- [Creating HTTP Cookie Sticky Groups, page 15-12](#)
- [Creating HTTP Header Sticky Groups, page 15-13](#)

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 <i>name1 name2</i>	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 <i>number1</i> [length <i>number2</i>]	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 <i>name</i>	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, page 15-14](#)
- [Configuring Layer 7 SIP Class Maps, page 15-14](#)
- [Configuring Layer 3 and Layer 4 Class Maps, page 15-15](#)
- [Configuring Management Class Maps, page 15-15](#)

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 <i>map_name</i>	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)# [<i>line_number</i>] match http url <i>expression</i> [method <i>name</i>]	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 <i>map_name</i>	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 <i>ip_address</i> [<i>mask</i>]	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 <i>header_name</i> header-value <i>expression</i>	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 <i>map_name</i>	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 <i>protocol_name</i> [any source_address <i>ip_address</i> <i>mask</i>]	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 Management Policy Maps, page 15-16](#)
- [Configuring Layer 7 Load Balancing Policy Maps, page 15-17](#)
- [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 <i>map_name</i>	Creates a policy map for management traffic.
Step 2	ACE_1/Admin(config-pmap-mgmt) # class <i>name1</i>	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 <i>map_name</i>	Creates a Layer 7 load-balancing policy map for HTTP traffic.
Step 2	ACE_1/Admin(config-pmap-lb) # class <i>name1</i>	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 <i>name</i>	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
```

**Note**

```
ACE_1/Admin(config-pmap-lb-c) # sticky-serverfarm WEB-STICKY
```

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 <i>map_name</i>	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 <i>name1</i>	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 <i>name</i>	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 <i>vlan</i> <i>vlan_number</i>	Enters configuration mode for the specified VLAN interface.
Step 2	ACE_1/Admin(config-if)# ip address <i>ip-address mask</i>	Configures the IP address and mask for the VLAN interface.
Step 3	ACE_1/Admin(config-if) # alias ip address <i>ip-address mask</i>	Defines the default route when a redundant ACE configuration exists. (Required only for redundant ACE configurations).

	Command	Purpose
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)# 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 6	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 7	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 8	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 9	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 10	ACE_1/Admin(config-ft-intf)# no shutdown	Enables the VLAN interface.
Step 11	ACE_1/Admin(config-ft-intf)# exit	Exits fault tolerant interface configuration mode.
Step 12	ACE_1/Admin(config)# ft peer peer_id	Configures an ACE local redundancy peer.
Step 13	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 14	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 15	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.
Step 16	ACE_1/Admin(config-ft-peer)# no shutdown	Enables the query interface.
Step 17	ACE_1/Admin(config-ft-peer)# exit	Exits fault-tolerant peer configuration mode.
Step 18	ACE_1/Admin(config)# ft group group_id	Creates a fault-tolerant group for redundancy.
Step 19	ACE_1/Admin(config-ft-group)# peer peer_id	Associates the peer with the fault-tolerant group.
Step 20	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.

	Command	Purpose
Step 21	ACE_1/Admin(config-ft-group) # priority <i>number</i>	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 22	ACE_1/Admin(config-ft-group) # associate-context <i>name</i>	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 23	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)# ip address 10.22.139.102 255.255.255.240
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)# ip address 10.22.139.113 255.255.255.240
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)# 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)# 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)# 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)# 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, page 15-22](#)
- [Configuring UDP Connection Timeout, page 15-23](#)
- [Enabling SysLog SIP Messages, page 15-23](#)
- [Configuring the Sticky Resource Class, page 15-23](#)
- [Assigning the Admin Context to the Sticky Resource Class, page 15-23](#)

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 than 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.
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 June 29, 2011

The following sections describe how to configure the Cisco TelePresence Multipoint Switch:

- [Configuring System Settings, page 16-1](#)
- [Configuring Unified CM Settings, page 16-5](#)
- [Configuring Cisco TelePresence Manager Settings, page 16-6](#)
- [Configuring Meeting Parameters, page 16-8](#)
- [Configuring Security Settings, page 16-11](#)

Additional information about Cisco TelePresence Multipoint Switch configuration is available at http://www.cisco.com/en/US/docs/telepresence/multipoint_switch/1_7/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, page 16-1](#)
- [Editing Route Pattern Settings, page 16-2](#)
- [Configuring QoS Settings, page 16-3](#)
- [Configuring Resource Management, page 16-4](#)
- [About SNMP Settings, page 16-4](#)

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. All of the settings on the Route Pattern window match the comparable field settings that you configure for the Cisco Unified Communications Manager (Unified CM).

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 as configured in Cisco Unified CM.
Route Pattern End	Defines the last number in your route pattern as configured in Cisco Unified CM.
Access Number	Displays the first number in the route pattern as defined in Cisco Unified CM. 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 ad hoc meetings. Note The access number cannot be used for static meetings.
Access Name	Descriptive name for the access number as defined in Cisco Unified CM. The maximum number of characters is 20.

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.
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 1.7 Administration Guide*, at http://www.cisco.com/en/US/docs/telepresence/multipoint_switch/1_7/administration/guide/CTMS_Release1_7.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, page 16-5](#)
- [Configuring SIP Profile Settings, page 16-6](#)

Configuring Unified CM Settings

You must configure an entry for each Unified CM server in the cluster. Additionally, you must configure an entry for each of the Cisco TelePresence Exchange System call engine servers, and configure an entry for the session border controller ingress interface.

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 Enter either the hostname or IP address of the two call engines of the Cisco TelePresence Exchange System in the first two fields. In the third field, enter the ACE virtual IP (VIP).
SIP Port	Port number for Cisco Unified SIP IP Phones that are using UDP to listen for SIP messages from Unified CM. The default setting is 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 Cisco TelePresence Manager Settings

The Cisco TelePresence Manager (CTS Manager) manages Cisco TelePresence Multipoint Switch resources for scheduled meetings.

This section describes the settings that are necessary to build the communication channel between the Cisco TelePresence Multipoint Switch and Cisco TelePresence Manager by using the Cisco TelePresence Multipoint Switch administration user interface.

Procedure

To configure Cisco TelePresence Manager settings, do the following procedure:

-
- Step 1** From the left navigation pane, choose **Configure > CTS Manager**.
A table with the CTS Manager configuration fields is displayed. [Table 16-5](#) describes the fields.
 - Step 2** Configure the CTS Manager settings as necessary, and then do one of the following:
 - To register new or modified settings, click **Apply**.
 - To restore the original settings, click **Cancel**.
-

Table 16-5 Cisco TelePresence Manager Settings

Field or Button	Setting
Description	Text describing or identifying this particular Cisco TelePresence Multipoint Switch. The maximum number of characters for this field is 62.
Time Zone	Indicates the time zone in which the Cisco TelePresence Multipoint Switch is located. CTS Manager uses this setting to identify the closest Cisco TelePresence Multipoint Switch for all scheduled Cisco TelePresence endpoints. Select the appropriate time zone from the Time Zone drop-down list.
User	Username that is used by Cisco TelePresence Multipoint Switch web services to communicate with CTS Manager. Note Usernames must be at least 5 characters, but not more than 64 characters in length, and can contain upper and lower case alphanumeric characters and the underscore and dash characters. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown. Note You must configure the same username and password on both the Cisco TelePresence Multipoint Switch and Cisco TelePresence Manager.
Password	Password that is used by Cisco TelePresence Multipoint Switch web services to communicate with CTS Manager. Note Passwords must be at least 5 characters, but not more than 64 characters in length, and can contain upper and lower case alphanumeric characters and the underscore and dash characters. Note You must configure the same username and password on both the Cisco TelePresence Multipoint Switch and Cisco TelePresence Manager.
Host	IP address or hostname of the Cisco TelePresence Manager.
Dial Plan	The following fields define the dialing system that the Cisco TelePresence Multipoint Switch and Cisco TelePresence Manager use to establish intercompany communication telepresence meetings.
Site Access Code	Defines the dialed numbers that are prepended to a Cisco TelePresence endpoint extension number to create a fully qualified domain name (FQDN) in a Cisco Unified CM cluster.
Inter Site Access Code	Defines the dialed prefix that is used to reach another site within the same company in a Cisco Unified CM cluster.
External Access Code	Defines the dialed prefix that is dialed from within a company to reach a local outside line.
National Dialing Digits	Defines the specific digits used to place a national call. For example, in the United States, the national dialing digit is 1.
International Dialing Digits	Defines the specific digits used to place an international call. For example, in the United States, the international dialing digits are 011.
Directory Number	The following fields define the E.164 numbering plan that is used for intercompany communication.

Table 16-5 Cisco TelePresence Manager Settings (continued)

Field or Button	Setting
Country Code	A unique set of digits that are used to identify a specific country as part of an E.164 number, as defined by the International Telecommunications Union (ITU). The country code can consist of 1, 2, or 3 digits.
National Destination Code	A unique set of digits that identify a specific national destination (area code) as part of an E.164 number, as defined by the International Telecommunications Union (ITU).
Local Number	A unique set of digits that identify a subscriber as part of an E.164 number, as defined by the International Telecommunications Union (ITU).
Registration Status	View only. Status of the registration between the Cisco TelePresence Multipoint Switch and the Cisco TelePresence Manager that is defined in the host entry.

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, page 16-8](#)
- [Creating Static Meetings, page 16-9](#)
- [Static Meeting Fields, page 16-10](#)

Configuring the Meet-Me User

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

To create the Meet-Me user and password, do the following procedure:

Step 1 From the left navigation pane, choose **Configure > Access Management**.

The Access Management window displays a summary of current users.

Step 2 To add a new user, click **New**.

The New User entry window appears.

Step 3 Enter **meetme** in the User Name field.



Note Beginning with Cisco TelePresence Exchange System Release 1.0(3), you can enter a user name of your choice rather than entering **meetme**.

Step 4 Enter **ciscotxbu** in the Password field.



Note Beginning with Cisco TelePresence Exchange System Release 1.0(3), you can enter a password of your choice rather than entering **ciscotxbu**.

- Step 5** To confirm the password, enter the password again.
- Step 6** Check the **Conference-Scheduler** role check box.
- Step 7** To save new or modified settings, click **Apply**.

Creating Static 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.



Note On the Cisco TelePresence MSE 8000 Series, static meetings are called permanent meetings. On the Cisco TelePresence Exchange System, static meetings are called standing meetings.

You must configure two separate ranges for static meetings and interop meetings. You do not need to configure interop meetings at this point; however, the parameters for configuring interop meetings are seen in [Table 16-6](#).



Note You must enter the same range of static meeting (and interop meeting numbers) 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 16-6](#) 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 16-6 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	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
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 .
Hosted Meeting	<p>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.</p> <p>Options are Yes and No. Click the appropriate radio button to select.</p>
Host Room Number	Defines the host Cisco TelePresence System room number.
Interop	<p>Determines whether the Cisco TelePresence Multipoint Switch handles interop meetings.</p> <p>Click the No radio button.</p> <p>Cisco TelePresence Server MSE 8710 and Cisco TelePresence MCU MSE 8510 manage interop meetings in the Cisco TelePresence Exchange Solution.</p> <p>Interop meetings include any standards-based H323 and ISDN endpoints.</p>

Table 16-6 Static Meeting Field Descriptions (continued)

Field or Button	Description
Quality	<p>This field sets the maximum default video quality for multipoint meetings:</p> <ul style="list-style-type: none"> • 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 <p>The default is Highest Detail, Best Motion: 1080p</p>
Meeting Security Policy	<p>Click the appropriate radio button to select:</p> <p>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.</p> <p>Non-Secure—Any Cisco TelePresence system can join the meeting.</p> <p>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.</p>

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, page 16-12](#)
- [Creating a SIP Trunk Security Profile, page 16-13](#)
- [Downloading CAPF Root Certificates from Unified CM, page 16-14](#)
- [Downloading Root Certificates from Unified CM, page 16-14](#)
- [Uploading CAPF Certificates, page 16-14](#)
- [Downloading LSC to Cisco TelePresence Multipoint Switch, page 16-15](#)
- [Setting Cisco TelePresence Multipoint Switch as Secure, page 16-15](#)

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 group, the Standard CTI Secure group, and the Standard CTS Secured Connection role under Permission Information.
 - 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 String—Enter the value of **123456**.
 - 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.

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	TCP will be entered automatically.
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.
Incoming Port	Yes	Enter 5060 for non-secure trunk. If using SIP security, enter a different unused port (such as 5275).

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**.
-

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 Names must be in the following format: CUCM#.der, where # is 0 for Publisher and 1 through 6 for Subscribers.

Uploading CAPF Certificates

Procedure

To upload CAPF 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 **Upload**.
 - 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**).
 - d. To upload the file onto the Cisco TelePresence Multipoint Switch, click **Upload**.
The newly uploaded file appears on the Security window.
-

Downloading LSC to Cisco TelePresence Multipoint Switch

Before You Begin

Create the application user and application user CAPF profile.

Upload the CAPF profile to the 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 created 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**.
After the LSC successfully downloads, the Cisco TelePresence Multipoint Switch reboots automatically.
-

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 > Cisco Unified CM**.
The Unified CM window is displayed.
 - Step 2** Click the **SIP Profile Settings** tab.
 - Step 3** From the Device Security drop-down list, select **Non-Secure**.
 - Step 4** From the Transport Layer Protocol drop-down list, choose **UDP**.
 - Step 5** To save your changes, click **Apply**.

Step 6 After reading the notice that is displayed, click **OK**.



CHAPTER 17

Configuring the Cisco Router with IVR

Revised June 29, 2011

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:

- [Downloading Application Files from the FTP Server, page 17-1](#)
- [Configuring the Router to Pass SIP Headers, page 17-2](#)
- [Configuring Application Parameters, page 17-2](#)
- [Configuring VOIP Dial Peers, page 17-3](#)

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 12.4T](#), at http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html.

Downloading Application Files from the FTP Server

To download the Meet-Me application file from the Cisco FTP Server, do the following procedure:

```
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.
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

Revised June 29, 2011

The procedures in this section address the minimum configuration requirements necessary on Cisco Unified Communications Manager (Unified CM):

- Create a SIP security profile. This security profile will be used on the SIP trunk between Cisco TelePresence Multipoint Switch and Unified CM.
- 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 Cisco TelePresence Multipoint Switch.

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, page 18-2](#)
- [Creating a SIP Trunk Security Profile, page 18-2](#)
- [Creating a SIP Trunk, page 18-3](#)
- [Associating the SIP Trunk with Route Patterns, page 18-3](#)
- [Deleting a Unified CM from the Cisco TelePresence Exchange System Administration Console, page 18-5](#)

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 *Unifed_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 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:
- From the Trunk Type drop-down menu, select **SIP Trunk**, and then click **Next**.
The Device Protocol field updates and displays SIP.
 - In the Device Name field, enter a name for the SIP trunk.
 - In the Description field, enter a description for the SIP trunk.
 - 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.
 - 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.
 - From the SIP Trunk Security Profile drop-down menu, select **Non Secure SIP Trunk Profile**.
 - From the SIP Profile drop-down menu, select **Standard SIP Profile**.
 - 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 Xs 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 18-2](#).

Table 18-2 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

Do the applicable procedure, depending on your Cisco TelePresence Exchange System version:

Procedure

To delete a Unified CM from Cisco TelePresence Exchange System Release 1.0(3), 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.

Procedure

To delete a Unified CM from Cisco TelePresence Exchange System Release 1.0(2) and earlier, do the following procedure:

-
- Step 1** From the navigation pane of the Cisco TelePresence Exchange System administration console, choose **Media Resources > CUCM Resources**.
- The CUCM Resources window is displayed.
- Step 2** Click the applicable **CUCM Resource** to go to the CUCM Resources page.
- Step 3** After verifying that you have chosen the correct CUCM resource to delete, click **Delete This CUCM Resource**, and then in the dialog box, click **OK** to confirm the deletion.
-



CHAPTER 19

Configuring Cisco TelePresence Manager

Revised June 29, 2011

This section describes the configuration steps necessary for the Cisco TelePresence Manager to communicate with the Cisco TelePresence Exchange System. This section includes the following topics:

- [Configuring Lightweight Directory Access Protocol Servers, page 19-1](#)
- [Configuring Unified CM, page 19-3](#)
- [Configuring the Scheduling API, page 19-5](#)
- [Adding Licenses, page 19-6](#)
- [Enabling Intercompany Calls, page 19-7](#)



Note

- 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 1.7 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_7/admin/ctm1_7adminguide.html.
-

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: <ul style="list-style-type: none"> 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. <p>Note To operate with the Cisco TelePresence Exchange System, select Normal.</p>
Port	Enter the applicable port given the configuration: <ul style="list-style-type: none"> The default port for a normal connection in a single LDAP server deployment is 389. The default port for a secure connection is 636. <p>Note To operate with the Cisco TelePresence Exchange System, use the default port value of 389.</p>
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 .
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=admin, 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.

Table 19-1 LDAP Server Settings (continued)

Field or Button	Description or Setting
User Containers	<p>Describes values for user and meeting room information that the Cisco TelePresence Manager retrieves from the LDAP Server.</p> <p>Additionally, these containers are used to retrieve user information for authentication from the LDAP server.</p> <p>You can specify more than one user container.</p> <p>Note If you have an LDAP peer domain configured, you need to specify its user containers and context.</p> <p>For example, cn=users, dc=domain2, dc=com.</p> <p>When specifying the container and context information for your peer domain, you do not check the Append default context box.</p>
Append default context	<p>Refers to a check box next to the Users Containers field.</p> <p>When you check the Append default context check box, it appends the default context to the User Container.</p> <p>Note To operate with Cisco TelePresence Exchange System, check the Append default context check box.</p>
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 Unified CM:

- [Creating an Application User, page 19-3](#)
- [Downloading the Certificate, page 19-4](#)
- [Uploading the Certificate to Cisco TelePresence Manager, page 19-5](#)

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.
- Include the user in the following groups in the Permission Information:
- Standard AXL API Access
 - Standard CTI Enabled
 - Standard Serviceability

- Standard CCM Admin Users

Step 4 To save your 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_0_2/secugd/sec-802-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 19-3.
Password	The password for the application user name.
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](#).
-

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: <ul style="list-style-type: none"> 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. <p>Note To operate with the Cisco TelePresence Exchange System, select Normal.</p>
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.
Test Connection	Tests the connection between the Cisco TelePresence Manager and the LDAP server. <p>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 on page 11-7.</p>

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. For example, if it is a room-to-room call it involves one room. If it is a multi-room call among three rooms, it is a triple call and you would provide the value of 3.

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

To enable intercompany features, do the following 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

Revised June 29, 2011

This section describes the Cisco TelePresence Exchange System configuration requirements for the session border controller (SBC) functionality.

This section includes the following topics:

- [Creating a Session Border Controller Interface, page 20-1](#)
- [Creating a Management Interface, page 20-2](#)
- [Creating the SBC Instance, page 20-2](#)
- [Configuring the Signaling Border Element, page 20-3](#)
- [Defining a Media Address, page 20-11](#)

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 <i>interface-number</i>	Creates a virtual SBC interface on the Cisco ASR.
Step 3	Router(config-if)# ip address <i>{IPv4 ip address} {IPv4 subnet address}</i>	Assigns a primary IP address and subnet mask to the SBC interface.
Step 4	Router(config-if)# ip address <i>{IPv4 ip address} {IPv4 subnet address} secondary</i>	(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 <i>module / slot / port</i>	Enters interface configuration mode for the specified interface.
Step 2	Router(config-if)# ip address <i>{IPv4 ip address} {IPv4 subnet address}</i>	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 <i>service-name</i>	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, adjacencies, call admission control policies, route tables and blacklists.

SBE configuration is described in the following sections:

- [Configuring Default Profiles, page 20-3](#)
- [Creating Adjacencies, page 20-5](#)
- [Configuring CAC Policy, page 20-7](#)
- [Configuring Call Policies, page 20-8](#)
- [Configuring SIP Timers, page 20-10](#)
- [Defining Blacklists, page 20-10](#)

Configuring Default Profiles

Procedure

To configure the default profiles on the SBE, do the following procedure:

	Command	Purpose
Step 1	Router(config)# sbc <i>service-name</i>	Enters SBC configuration mode for the specified SBC instance.
Step 2	Router(config-sbc)# sbe	Enters SBE configuration mode.
Step 3	Router(config-sbc-sbe)# sip-header profile <i>profile-name</i>	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.

	Command	Purpose
Step 4	Router(config-sbc-sbe-sip-hdr)# header <i>header-name</i>	Adds the specified header to the profile.
Step 5	Router(config-sbc-sbe-sip-hdr- le)# 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 to pass , which allows the message to proceed.
Step 6	Router(config-sbc-sbe-sip-hdr- le)# exit Router(config-sbc-sbe-sip-hdr)# exit	Exits the header profile configuration mode.
Step 7	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 8	Router(config-sbc-sbe-sip-mth)# pass-body	Permits SIP message bodies to pass through.
Step 9	Router(config-sbc-sbe-sip-mth)# method <i>method-name</i>	Adds a method with a specified name to a SIP message profile.
Step 10	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 11	Router(config-sbc-sbe-sip-mth)# exit	Exits the method profile configuration mode.
Step 12	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 13	Router(config-sbc-sbe-sip-opt)# option <i>opt-name</i>	Adds an option to the profile.
Step 14	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-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 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-expiry 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 pass
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 INVITE
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 REPLACES
Router(config-sbc-sbe-sip-opt)# exit

```

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 SP 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) <i>adjacency-name</i>	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)# hunting-trigger <i>error-codes</i>	Configures SIP to retry routing to the adjacency if it receives one of the specified error codes.
Step 4	Router(config-sbc-sbe-adj-sip)# preferred-transport {tcp udp}	Sets the preferred transport protocol for SIP signaling on the adjacency.

	Command	Purpose
Step 5	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 6	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 7	Router(config-sbc-sbe-adj-sip)# statistics-setting summary	Enables the show sbc sbe sip-method-stats command to display a summary level of statistics about SIP request names.
Step 8	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.
Step 9	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 10	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)# 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-setting 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)# 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)# 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
```


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 <i>policy-set-id</i>	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 <i>table-name</i>	Defines the first policy table to process when performing the admission control stage of policy.
Step 3	Router(config-sbc-sbe-cacpolicy)# cac-table <i>table-name</i>	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 <i>entry-id</i>	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.
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 <i>policy-set-id</i>	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 <i>policy-set-id</i>	Creates a new policy set for processing calls within the SBE.
Step 2	Router(config-sbc-sbe-rtgpolicy)# first-call-routing-table <i>table-name</i>	Configures the name of the first routing table for new-call events.
Step 3	Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table <i>table-id</i>	Creates a new routing table whose entries match the source adjacency.
Step 4	Router(config-sbc-sbe-rtgpolicy -rtgtable)# entry <i>entry-id</i>	Creates an entry in the routing table.
Step 5	Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# action { complete { next-table <i>go-to-table-name</i> } }	Specifies the next routing table to process if the event matches the entry. Action complete specifies that no further action is required.
Step 6	Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# edit-cic replace <i>ds</i>	Replaces the carrier ID in the SIP message with the specified digit string.
Step 7	Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# dst-adjacency <i>target-adjacency</i>	Configures the destination adjacency for calls that match this table entry.
Step 8	Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# match-adjacency <i>key</i>	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 <i>table-id</i>	Creates a new routing table whose entries match the carrier ID field.
Step 12	Router(config-sbc-sbe-rtgpolicy -rtgtable)# entry <i>entry-id</i>	Creates an entry in the routing table.
Step 13	Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# action { complete { next-table <i>go-to-table-name</i> } }	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 <i>ds</i>	Replaces the carrier ID in the SIP message with the specified digit string.

	Command	Purpose
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 <i>interval</i>	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 <i>interval</i>	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 <i>event</i>	Configures the event type for which SBC applies the limit.
Step 3	Router(config-sbc-sbe-blacklist -global-reason)# timeout <i>number</i> { 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.

	Command	Purpose
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)# sb c <i>service-name \</i>	Enters SBC configuration mode for the specified SBC instance.
Step 2	Router(config-sbc)# media-address ipv4 <i>IPv4 ip</i> <i>address</i>	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 <i>min-port max-port any</i>	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 <i>min-port</i> value is 16384, the default <i>max-port</i> 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 <i>timeout</i>	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

Revised June 29, 2011

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, page 21-1](#)
- [Configuring Cisco TelePresence MSE 8000 Series Settings, page 21-2](#)
- [Configuring Call Control, page 21-10](#)

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 either the 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 Cisco TelePresence Exchange System does not require any specific configuration settings on the Cisco VCS. The required media resources and ISDN gateways register directly with the Cisco VCS.
- However, there are some configuration settings that must be made on the SBC that is use within the network. For details see the [“Configuring Cisco VCS Settings” section on page 21-11](#).
- For more 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 supervisor module and the optional service modules:

- [Accessing the Web Interface, page 21-2](#)
- [Configuring SNMP Traps, page 21-2](#)
- [Configuring Cisco TelePresence Server MSE 8710 Settings, page 21-3](#)
- [Configuring Cisco TelePresence MCU MSE 8510 Settings, page 21-5](#)
- [Configuring Cisco TelePresence ISDN GW MSE 8321 Settings, page 21-7](#)

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, page 21-3](#)
- [Configuring H.323 Gatekeeper, page 21-4](#)
- [Configuring API User, page 21-4](#)

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.

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.

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, page 21-5](#)
- [Configuring SNMP Traps, page 21-6](#)
- [Configuring Conference Settings, page 21-6](#)
- [Configuring Media Port Settings, page 21-6](#)
- [Configuring H.323 Settings, page 21-7](#)
- [Configuring API User, page 21-7](#)

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.
-

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, page 21-8](#)
- [Configuring SNMP Traps, page 21-8](#)
- [Configuring ISDN Settings, page 21-8](#)
- [Configuring ISDN Ports, page 21-9](#)

- [Configuring H.323 Settings, page 21-9](#)
- [Configuring IP to ISDN Dial Plan, page 21-10](#)

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.

See the following sections for additional details:

- [Configuring Cisco VCS Settings, page 21-11](#)
- [Configuring H.323 Gateway Settings on the SBC, page 21-11](#)

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 Cisco TelePresence Exchange System does not require any specific configuration settings on the Cisco VCS. The required media resources and ISDN gateways register directly with the Cisco VCS. However, there are some configuration settings that must be made on the SBC that is use within the network.

For more 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 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 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 21-11](#)
- [Configuring Call Policies, page 21-12](#)

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.
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.

	Command	Purpose
Step 7	Router(config-sbc-sbe-adj-h323)# tech-prefix <i>prefix-num</i>	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 <i>policy-set-id</i>	Creates a new policy set for processing calls within the SBE.
Step 2	Router(config-sbc-sbe-rtgpolicy)# first-call-routing-table <i>table-name</i>	Configures the name of the first routing table for new-call events.
Step 3	Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table <i>table-id</i>	Creates a new routing table whose entries match the source adjacency.
Step 4	Router(config-sbc-sbe-rtgpolicy- -rtgtable)# entry <i>entry-id</i>	Creates an entry in the routing table.
Step 5	Router(config-sbc-sbe-rtgpolicy- -rtgtable-entry)# match-adjacency <i>key</i>	Configures the source adjacency as the match value for this table entry.

	Command	Purpose
Step 6	Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action { complete { next-table <i>go-to-table-name</i> } }	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 <i>ds</i>	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 <i>table-id</i>	Creates a new routing table whose entries match the source adjacency.
Step 11	Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry <i>entry-id</i>	Creates an entry in the routing table.
Step 12	Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address <i>key</i>	Configures the carrier ID match value of the entry.
Step 13	Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency <i>target-adjacency</i>	Configures the destination adjacency of an entry in a routing table.
Step 14	Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action { complete { next-table <i>go-to-table-name</i> } }	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 <i>ds</i>	Replaces the carrier ID in the SIP message with the specified digit string.
Step 16	Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency <i>target-adjacency</i>	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 <i>policy-set-id</i>	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-rtgppolicy-rtgtable-entry)# action next-table OUTGOING
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# exit

Router(config-sbc-sbe-rtgppolicy)# rtg-dst-address-table OUTGOING
Router(config-sbc-sbe-rtgppolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# match-address 1922 digits
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgppolicy-rtgtable)# entry 2
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# match-address 1922 digits
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# edit-dst del-prefix 1
Router(config-sbc-sbe-rtgppolicy-rtgtable)# entry 3
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# match-address 139 digits
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgppolicy-rtgtable-entry)# prefix
Router(config-sbc-sbe-rtgppolicy-rtgtable)# exit
Router(config-sbc-sbe-rtgppolicy)# complete
Router(config-sbc-sbe-rtgppolicy)# exit
Router(config-sbc-sbe)# active-call-policy-set 1
```



CHAPTER 22

Configuring Internet Group Management Protocol for Multicast Support

Revised June 29, 2011

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, multicasting between the two call engines.

Additionally, the chapter provides multicast configuration recommendations for non-Cisco switches, and includes the following topics:

- [Multicasting Overview, page 22-1](#)
- [Configuring the IGMP Querier Functionality on a Cisco Switch, page 22-2](#)
- [Configuring PIM on a Cisco Router, page 22-4](#)
- [Configuring IGMP on a Non-Cisco Switch, page 22-6](#)

Multicasting Overview

The Cisco TelePresence Exchange System employs multicasting 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 not 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 <i>vlan_ID</i>	Selects the VLAN in which the switch and the call engines operate.
Step 3	Router(config-if)# ip address <i>ip_address subnet_mask</i>	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 <i>vlan vlan_ID</i> 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 <i>vlan_ID</i>	Selects the VLAN in which the switch and the call engines operate.

	Command	Purpose
Step 3	Router(config-if)# ip address <i>ip_address subnet_mask</i>	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 <i>vlan_ID</i> 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 <i>vlan_ID</i> querier address <i>ip_address</i>	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 <i>vlan_ID</i>	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 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 <i>vlan_ID</i>	Selects the VLAN in which the router and the call engine VLAN operate.
Step 3	Router(config-if)# ip address <i>ip_address subnet_mask</i>	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 <i>vlan vlan-id</i> [neighbor mac-group statistics mroute [<i>source-ip</i> <i>group-ip</i>]]	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 2/3 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 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 configuration guidelines listed below:

- 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, do the following task:
 - 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.



PART 5

Maintaining the Cisco TelePresence Exchange System

- [Managing Database Backups](#)
- [Meeting Diagnostics](#)
- [Advanced Configuration](#)
- [Configuring SNMP](#)
- [Configuring Cisco Discovery Protocol](#)
- [Changing the Network Configurations](#)



CHAPTER 23

Managing Database Backups

Revised June 29, 2011

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, page 23-1](#)
- [Viewing Past Database Server Backups and Restores, page 23-1](#)
- [Performing a Manual Database Backup, page 23-3](#)
- [Restoring a Database Server Backup, page 23-4](#)

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:

- Start time of the backup
- Date of the backup file that is restored on the database server
- 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 Manual 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

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.

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 24

Meeting Diagnostics

Revised June 29, 2011

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, page 24-1](#)
- [Viewing Meeting Diagnostics \(Cisco TelePresence Exchange System Release 1.0\(3\) and Later Only\), page 24-2](#)
- [Viewing Meeting Diagnostics \(Cisco TelePresence Exchange System Release 1.0\(2\) and Earlier Only\), page 24-5](#)

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
- 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 **Cancel**.

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.

Viewing Meeting Diagnostics (Cisco TelePresence Exchange System Release 1.0(3) and Later Only)

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); the reserved and available capacity for each resource; and Call Detail Records (CDRs) for each meeting.
- **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.

For a detailed list of the fields on the Meeting Diagnostics page, see [Table 24-1](#).

For instructions on viewing meeting diagnostics, see the [“Procedure” section on page 24-4](#).

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 \(Cisco TelePresence Exchange System Release 1.0\(3\) and Later Only\)” section on page 24-4](#).

Table 24-1 Meeting Diagnostics Field Descriptions

Field	Description
Participants View Tab	
Resources Used Table	
Resource Name	A link to the management site of the resource.
Location	A text string indicating the region of the resource.
Reserved Capacity	The number of segments reserved by Cisco TelePresence Exchange System for the resource.
Available Capacity	The number of segments available for the resource.
Participants Currently in the Meeting Table	
Time	Time and date stamp indicating when the participant joined the meeting.

Table 24-1 Meeting Diagnostics Field Descriptions (continued)

Field	Description
Description	Text string indicating whether the participant dialed in, or was connected to the meeting by dial out from the Cisco TelePresence Exchange System.
Endpoint	Text string indicating whether the endpoints are provisioned or unprovisioned.
Ports	The number of ports assigned to the endpoint.
CDR	A link to the call detail record.
Dial-In/Dial-Out	Text string indicating whether the participant is a dial-in or dial-out call.
Details	A link to a page that provides additional details.
Participants Not in the Meeting Table	
Participant	The access number of the participant.
Join Time	Time and date stamp indicating when the participant joined the meeting.
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/Dial Out in Progress	A button that toggles between Redial and Dial Out in Progress. When you click the Redial button to reconnect a disconnected participant, the button text changes to Dial Out in Progress. Note When the meeting has ended, the Redial button is dimmed.
Events View Tab	
Meeting Events Table	
Time	Chronological list of time and date stamps associated with meeting events.
Description	Text descriptions detailing each event that occurs, for example: <ul style="list-style-type: none"> • Meeting Ended • Meeting Started • Meeting Resources Reserved
Details	A link to a page that provides additional details.
Alarms Near Meeting Time Table	
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.
Summary	Text description of the alarm.
Server	Name of the server on which the alarm occurred.

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.
- Step 3** From the toolbar, click **Go to Diagnostics**.
The Meeting Diagnostics page is displayed.
-

**Note**

For information on viewing Meeting Diagnostics in Cisco TelePresence Exchange System Release 1.0(2) and earlier, see the [“Viewing Meeting Diagnostics \(Cisco TelePresence Exchange System Release 1.0\(2\) and Earlier Only\)”](#) section on page 24-5.

Reconnecting Disconnected Meeting Participants to a Meeting (Cisco TelePresence Exchange System Release 1.0(3) and Later Only)

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.

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 Participants Not in the Meeting table, in the Redial Participant column, click **Redial** to reconnect the applicable participant.

After you click Redial, the Redial button changes to **Dial Out in Progress**. The system dials out to the endpoint, and gives the endpoint three opportunities to pick up. When the endpoint picks up, the participant reappears in the Participants Currently in the Meeting table. Reconnecting a disconnected participant may take up to 30 seconds.

**Note**

If the meeting in question occurred in the past, participants listed in the Participants Not in the Meeting table cannot be reconnected to the meeting; thus the Redial button will be dimmed.

Step 5 To return to the Meetings page, from the toolbar, click **Meeting Details Page**.

Viewing Meeting Diagnostics (Cisco TelePresence Exchange System Release 1.0(2) and Earlier Only)

Meeting diagnostics allows the administrator to view details about a meeting.

There are two Meeting Diagnostic views:

- **Participants view**—Summarizes those participants currently (and previously) involved in the meeting and 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 that resource. Additionally, you can view Call Detail Records (CDRs) for each meeting.
- **Meeting View**—Provides a chronological summary of all events that occur from the time a meeting is scheduled to the time the meeting is completed.

**Note**

For information on viewing Meeting Diagnostics in Cisco TelePresence Exchange System Release 1.0(3) and later, see the [“Viewing Meeting Diagnostics \(Cisco TelePresence Exchange System Release 1.0\(3\) and Later Only\)”](#) section on page 24-2.

Procedure

To view meeting details, do the following procedure:

Step 1 From the navigation pane, choose **Diagnostics > Meetings Diagnostics**.

Step 2 Enter the Conference ID of the meeting for which you want to find details in to the search field, and then click **Search**.

You can find the Conference ID for a meeting by choosing either **Collaboration Services > Meetings** or **Collaboration Services > Standing Meetings**, and then clicking a specific meeting entry from the Subject column to display the Meetings Overview window.

From the Meetings Overview window, you can also launch the Meeting Diagnostics windows for that meeting by clicking **Go to Diagnostics**.



CHAPTER 25

Advanced Configuration

Revised June 29, 2011

The Advanced Configuration window in the administration console allows the administrator to define a prefix value for all ISDN guest dial out calls, and to define the external HTTP load-balancing address for the SIP engines, when the ACE is in use within the network.

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

- [Configuring an ISDN Dial Out Prefix, page 25-1](#)
- [Configuring a Meet-Me External HTTP Address, page 25-2](#)
- [Application Parameter Fields, page 25-2](#)
- [Deleting an Application Parameter, page 25-3](#)

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 prefix to determine whether to send the call to the ISDN gateway. If the configured ISDN 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 dial out prefix is 9. The administrator can modify the default ISDN dial out 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.

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 **Advanced Parameters > Application Parameters**.
The Application Parameters window is displayed.
 - Step 2** Click **Add a New Application Parameter**.
 - Step 3** In the entry window that is displayed, enter settings for the ISDN dial out prefix.
[Table 25-1](#) describes the fields.

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

Configuring a Meet-Me External HTTP Address

The administrator defines the Meet-Me external HTTP load-balancing address for call engines that employ the ACE for redundancy. Generally, the administrator defines the Meet-Me external HTTP 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 Meet-Me External HTTP Address, do the following procedure:

- Step 1** From the navigation pane, choose **Advanced Parameters > Application Parameters**.
The Application Parameters window is displayed.
- Step 2** Click **Add a New Application Parameter**.
- Step 3** In the entry window that is displayed, enter settings for the Meet-Me External HTTP Address.
[Table 25-1](#) describes the fields.
- Step 4** To save your changes, click **Save**.

Application Parameter Fields

Table 25-1 Application Parameter Field Descriptions

Field	Description
Parameter	Drop-down list. Choose the advanced configuration option that you are configuring from the drop-down list. Options are: <ul style="list-style-type: none"> ISDN Dialout Prefix Meet-Me External HTTP Address <p>Note By default, the ISDN dial out prefix setting is 9. You do not need to modify this value when it matches the setting in the Cisco VCS.</p>
Value	Text field. Enter the prefix number value that the system must append to the number to define the application (such as ISDN call or Meet-Me call). <p>Note By default, the ISDN dial out prefix setting is 9. There is no need to modify this value when it matches the setting in the Cisco VCS.</p>
Application	Text field. Enter the name of the application (such as ISDN dial out call or Meet-Me call).

Deleting an Application Parameter

Procedure

To delete an application parameter, do the following procedure:



Note At the end of the procedure, you may need to restart the system in order for your changes to take effect.

Step 1 From the navigation pane, choose **Advanced Configuration > Application Parameters**.

The Application Parameters window is displayed.

Step 2 Do the following sub-steps, depending on your Cisco TelePresence Exchange System version.

Cisco TelePresence Exchange System Release 1.0(3)

- a. In the item table, check the check box next to the entry that you want to delete. You can delete multiple application parameters 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.

Cisco TelePresence Exchange System Release 1.0(2) and earlier

- a. In the item table, check the check box next to the entry you want to delete.
- b. From the drop-down list that appears, choose **Delete**.
- c. Click **Go**.
- d. In the panel that is displayed to confirm the deletion, click **OK**.



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



CHAPTER 26

Configuring SNMP

Revised June 29, 2011

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, page 26-1](#)
- [Supported MIBs, page 26-2](#)
- [About SNMP on the Cisco TelePresence Exchange System, page 26-2](#)
- [How to Configure SNMP, page 26-4](#)

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, 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	<ul style="list-style-type: none"> • Cisco Session Border Controller • Cisco TelePresence Multipoint Switch • Cisco router with IVR¹ • Cisco TelePresence ISDN GW MSE 8321 	15 seconds	SIP OPTIONS PING
XML-RPC-based resources	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Adding SNMP Users, page 26-4 • Adding SNMP Trap Destinations, page 26-6
Remove SNMP configurations.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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} [passphrase]`



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 = 0x8000DEEC AFE8111BEEFADE
```

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

- If SNMP does not work as expected, complete the following tasks on the problematic Cisco TelePresence Exchange System server. If the problem is not specific to one server, complete these tasks on all nodes in the server cluster.
 1. [Verifying that the SNMP Service is Running, page 26-12](#)
 2. [Restarting the SNMP Service, page 26-13](#)
- You can also 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.

Verifying that the SNMP Service is Running

By default, the SNMP service automatically runs on each Cisco TelePresence Exchange System server. Complete this task only if you previously stopped services on the server or find that queries do not work after configuring SNMP.

Procedure

Step 1 Log in to the CLI of the server.

Step 2 Enter `utils service list`.

```

admin: utils service list

Requesting service status, please wait...
System SSH [STARTED]
Cluster Manager [STARTED]
SNMP [STARTED]

```

Step 3 Confirm that the SNMP service has started.

If the SNMP service has not started, proceed to the “[Restarting the SNMP Service](#)” section on page 26-13.

Restarting the SNMP Service

Complete this task only if SNMP is not working for some reason on a Cisco TelePresence Exchange System server.

Procedure

- Step 1** Log in to the CLI of the server.
 - Step 2** Enter **utils service stop SNMP**.
 - Step 3** Enter **utils service start SNMP**.
 - Step 4** Proceed to the [“Verifying that the SNMP Service is Running”](#) section on page 26-12.
-



Tip

The commands that start and stop services are case-sensitive.



CHAPTER 27

Configuring Cisco Discovery Protocol

Revised June 29, 2011

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, page 27-1](#)
- [Displaying the CDP Configuration, page 27-2](#)

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

---

### Revised June 29, 2011

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, page 28-1](#)
- [Changing the Database VIP Address That Is Configured on a Call Engine or Administration Server, page 28-4](#)
- [Configuring SIP Load Balancing on the Call Engine Servers, page 28-5](#)
- [Changing the IMM Interface Configuration, page 28-7](#)

## 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
 *** WARNING ***
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 20-5.
  - Cisco Unified Communications Manager configuration on the Cisco TelePresence Multipoint Switch. See the [“Configuring Unified CM Settings”](#) section on page 16-5.
  - 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 18-3.
- 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 5-22.

## 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:
- Stop the call engine server by entering the **utils service sipserver stop** command.

```
admin: utils service sipserver stop
sipserver.....Stopped
```
 - Start the call engine server by entering the **utils service sipserver start** command.

```
admin: utils service sipserver start
sipserver.....Starting - PID <32367>
```
 - 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 difference 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

- [Password Recovery](#)
- [Split Brain Recovery](#)
- [Corrupted MySQL Database Recovery](#)
- [Troubleshooting Calls](#)
- [Server Failure Recovery](#)
- [Logs](#)



CHAPTER 29

Password Recovery

Revised June 29, 2011

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

- 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.

- 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

Revised June 29, 2011

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 the current primary database server loses power, or its integrated management module (IMM) becomes unreachable by the secondary database server (for example, due to network connectivity issues), the secondary database server cannot automatically take over as primary. If the current primary database server fails under these conditions, your system may or may not enter split brain mode. In this situation, take one of the following actions:

- If the primary database server comes back up, the system may enter split brain mode; proceed to the [“Diagnosing Split Brain Mode”](#) section on page 30-1.
- If the primary database server remains down, the split brain recovery procedure is not applicable; instead, see the [“Recovering from a Failed Primary Database Server”](#) section on page 33-1.

This chapter includes the following topics:

- [Diagnosing Split Brain Mode](#), page 30-1
- [Recovering from Split Brain Mode](#), page 30-3
- [Verifying Synchronization of the Database Servers](#), page 30-4
- [Diagnosing Corrupted DRBD Metadata](#), page 30-6
- [Recovering from Corrupted DRBD Metadata](#), page 30-7

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 one or more of the following conditions, the database servers are in split brain mode:
- The connection state (cs) is “StandAlone.”
 - The role (ro) values display one of the following combinations:
 - “Primary/Unknown” on one server and “Secondary/Unknown” on the other server.
 - “Secondary/Secondary” on both servers—In this particular case, if the connection state (cs) 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, the connection state (cs) of 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
The database primary node name                 : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name               : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Running pid 2820
MySQL status                                   : Running pid 2810
Heartbeat status                              : Running pid 3752
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res   cs      ro      ds      p      mounted  fstype
0:mysql StandAlone Primary/Unknown UpToDate/DUnknown r----  ext3
-----
```

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
The database primary node name                 : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name               : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Running pid 10183
MySQL status                                   : Running pid 10100
Heartbeat status                               : Running pid 20414
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res      cs      ro      ds      p  mounted  fstype
...      sync'ed:  2.0%      (44104/44980)M
0:mysql    SyncSource Primary/Secondary UpToDate/Inconsistent C /mnt/mysql ext3
-----
```

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
The database primary node name                 : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name               : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Not running (only runs on primary)
MySQL status                                   : Not running (only runs on primary)
Heartbeat status                               : Running pid 17842
-----
```

```
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res  cs          ro          ds          p mounted  fstype
...    sync'ed:    2.1%          (44060/44980)M
0:mysql SyncTarget Secondary/Primary Inconsistent/UpToDate C
-----
```



Note The synchronization takes approximately 40 minutes. During this time, the disk state (ds) 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 state (ds) 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
The database primary node name                  : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name                : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Running pid 10183
MySQL status                                   : Running pid 10100
Heartbeat status                               : Running pid 20414
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res  cs          ro          ds          p mounted  fstype
0:mysql Connected Primary/Secondary UpToDate/UpToDate C /mnt/mysql ext3
-----
```

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
The database primary node name                  : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name                : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Not running (only runs on primary)
MySQL status                                   : Not running (only runs on primary)
Heartbeat status                               : Running pid 17842
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res  cs          ro          ds          p mounted  fstype
0:mysql Connected Secondary/Primary UpToDate/UpToDate C
-----
```

**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 state (ds) value is “Inconsistent/Inconsistent” while the connection state (cs) 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 30-7.
-

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
The database primary node name                 : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name               : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Not running (only runs on primary)
MySQL status                                   : Not running (only runs on primary)
Heartbeat status                               : Running pid 11459
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res    cs          ro          ds          p  mounted  fstype
0:mysql  WFConnection Secondary/Unknown Inconsistent/Inconsistent C
-----
```

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

Revised June 29, 2011

This chapter includes the following sections:

- [Diagnosing a Corrupted MySQL Database, page 31-1](#)
- [Recovering from a Corrupted MySQL Database, page 31-2](#)

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 state (cs) is “Connected.”
 - The disk state (ds) value is “Inconsistent/Inconsistent.”
 - The role (ro) 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  
The database primary node name                  : ctx-db-1  
The database primary node IP address            : 10.22.130.49
```

```

The database secondary node name           : ctx-db-2
The database secondary node IP address     : 10.22.130.57
Mon status                                 : Not running (only runs on primary)
MySQL status                               : Not running (only runs on primary)
Heartbeat status                           : Running pid 19984
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res   cs      ro      ds      p  mounted  fstype
0:mysql Connected Secondary/Secondary UpToDate/UpToDate C
-----

```

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 23-3.



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 23-4](#).



CHAPTER 32

Troubleshooting Calls

Revised June 29, 2011

This chapter describes issues with troubleshooting calls, and includes the following topics:

- [Troubleshooting Interop Calls, page 32-1](#)
- [Troubleshooting Failure of an Endpoint to Call into a Second Meeting, page 32-4](#)

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.

Do the applicable procedure, depending on your version of Cisco TelePresence Exchange System:

- [Troubleshooting an Interop Call in Cisco TelePresence Exchange System Release 1.0\(3\) and Later, page 32-1](#)
- [Troubleshooting an Interop Call in Cisco TelePresence Exchange System Release 1.0\(2\), page 32-2](#)

Troubleshooting an Interop Call in Cisco TelePresence Exchange System Release 1.0(3) and Later

Procedure

To troubleshoot an interop call in Cisco TelePresence Exchange System Release 1.0(3) and later, 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 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 an Interop Call in Cisco TelePresence Exchange System Release 1.0(2)

Procedure

To troubleshoot an interop call in Cisco TelePresence Exchange System Release 1.0(2), do the following procedure:

Step 1 Log in to the Cisco TelePresence Exchange System.

Step 2 From the navigation pane, choose **Diagnostics > Meetings Diagnostics**.

The Meeting Diagnostics window is displayed.

- Step 3** In the search field, enter the Conference ID of the meeting that is experiencing connection problems and click **Search**.

You can find the Conference ID for a meeting by choosing either **Collaboration Services > Meetings** or **Collaboration Services > Standing Meetings**, and then clicking a specific meeting entry from the Subject column to display the Meetings Overview window.

From the Meetings Overview window, you can also go directly to the Meeting Diagnostics windows for that meeting by clicking the **Go to Diagnostics** button (top).

- Step 4** 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 5** Log in to the Cisco VCS as the administrator.

- Step 6** From the tool bar, choose **Status > Calls > History**.

The Call History window is displayed.

- Step 7** 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 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.



Server Failure Recovery

Revised June 29, 2011

This chapter includes the following sections:

- [Recovering from a Failed Primary Database Server, page 33-1](#)
- [Replacing a Database Server, page 33-4](#)
- [Replacing an Administration or Call Engine Server, page 33-9](#)

Recovering from a Failed Primary Database Server

If the current primary database server and its integrated management module (IMM) lose power or otherwise fail, the current secondary server cannot automatically take over the primary role. Under these conditions, all calls to or from the system fail, and meetings cannot be scheduled or modified.

To avoid this situation, see the “[Power Recommendations for High Availability of the Database Servers](#)” section on page 4-3.

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, page 33-1](#)
- [Enabling HA After Recovering a Database Server, page 33-3](#)

Disabling High Availability to Enable the Current Secondary Database Server to Take Over the Primary Role

The high availability (HA) implementation requires access to the IMM of the failed node to ensure that the node is no longer accessing the Distributed Replicated Block Device (DRBD) disk, which is a shared resource, before allowing a role transfer. Therefore, if the IMM interface of the current primary database server becomes unavailable, you need to complete the following procedure to manually enable the current secondary database server to take over the primary role.

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
The database primary node name                 : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name               : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Not running (only runs on primary)
MySQL status                                   : Not running (only runs on primary)
Heartbeat status                              : Running pid 17337
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res    cs          ro          ds          p mounted  fstype
0:mysql  WFCnection  Secondary/Unknown  UpToDate/DUnknown  C
-----

```



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 33-4.

Step 3 Enter **utils service database drbd disable-ha**.

```

admin: utils service database drbd disable-ha
Stopping Heartbeat...
Disabling STONITH...
[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
The database primary node name                 : ctx-db-1
The database primary node IP address           : 10.22.130.49
The database secondary node name               : ctx-db-2
The database secondary node IP address         : 10.22.130.57
Mon status                                     : Running pid 20494
MySQL status                                 : Running pid 20445
Heartbeat status                              : Running pid 18030
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res    cs          ro          ds          p mounted  fstype
0:mysql  WFCnection  Primary/Unknown  UpToDate/DUnknown  C /mnt/mysql  ext3
-----

```

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, for example, by reconnecting its power cable or fixing its power source.

- 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 33-4](#).

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 33-4](#).



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
Stopping Heartbeat...
Stopping Mon...
Stopping mon daemon: [ OK ]
Stopping MySQL...
Shutting down MySQL. SUCCESS!
Unmounting DRBD Volume...
Entering DRBD Secondary mode...
Enabling STONITH...
Starting Heartbeat...
[Done]
```

Step 4 Turn on the recovered server but do not take any further actions on that server.

After the IMM becomes available, the HA implementation will automatically set up the peer communications and reboot the recovered node.

- Step 5** 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 and Synchronizing the Replacement for the Initial Secondary Database Server](#), page 33-6
- [Installing the Software on and Synchronizing the Replacement for the Initial Primary Database Server](#), page 33-7

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 Make sure 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. To simplify management, Cisco recommends that you use the same username and password on all Cisco TelePresence Exchange System servers.
- 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.

- Network and access information for the integrated management module (IMM) interface, which is required to implement active/standby redundancy for the database servers, and which enables remote control of the individual database server:
 - IP address and subnet mask.
 - Default gateway.
 - Username and password.
- 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.
- (Optional) Domain Name System (DNS) information:
 - IP address of a primary DNS server.
 - (Optional) IP address of a secondary DNS server.
 - Domain name.

Setting Up the Replacement Database Server

Before You Begin

Complete the procedure in the [“Replacing a Database Server”](#) section on page 33-4.

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 the following sections:
- [Power Recommendations for High Availability of the Database Servers](#), page 4-3
 - [Cabling Requirements for the Database Servers](#), page 4-3
- Step 3** Set up the IMM interface, which is required to implement active/standby redundancy for the database servers. 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 and Synchronizing the Replacement for the Initial Secondary Database Server, page 33-6](#)
 - [Installing the Software on and Synchronizing the Replacement for the Initial Primary Database Server, page 33-7](#)
-

Installing the Software on and Synchronizing 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 Role of the Database Servers”](#) section on page 5-8.

- Step 3** Turn off the replacement server.

- Step 4** Log in to the CLI of the current primary database server.

- Step 5** Enter **utils service database drbd enable-ha**.

```
admin: utils service database drbd enable-ha
Stopping Heartbeat...
Stopping Mon...
Stopping mon daemon: [ OK ]
Stopping MySQL...
Shutting down MySQL. SUCCESS!
Unmounting DRBD Volume...
Entering DRBD Secondary mode...
Enabling STONITH...
Starting Heartbeat...
[Done]
```

- Step 6** Turn on the replacement server.

- Step 7** Log in to the CLI of the replacement server.

Step 8 Enter **utils service database sync**.

Step 9 Log in to the CLI of the current primary database server.

Step 10 Enter **utils service database drbd keep-node**.

```
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 11 Proceed to the [“Verifying Synchronization and Network Connectivity of the Database Servers”](#) section on page 5-12.

Related Topics

- [Command Reference, page C-1](#)

Installing the Software on and Synchronizing the Replacement for the Initial Primary Database Server

Before You Begin

Complete the procedure in the [“Replacing a Database Server”](#) section on page 33-4.



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
Unable to run CLI as root due to unsuccessful service drbd status!
-----
The initial configured HA role of this node      : primary
The current HA role of this node                  :
The database vip address                          : 10.22.130.54
The database primary node name                    : ctx-db-1
The database primary node IP address              : 10.22.130.49
The database secondary node name                  : ctx-db-2
The database secondary node IP address            : 10.22.130.57
Unable to run CLI as root due to unsuccessful service heartbeat status!
Mon status                                        : Not running (only runs on primary)
MySQL status                                       : Not running (only runs on primary)
```

```
Heartbeat status : Not running
-----
```

```
Executed command unsuccessfully
```

Step 3 Turn off the replacement server.

Step 4 Log in to the CLI of the current primary database server.

Step 5 Enter **utils service database drbd enable-ha**.

```
admin: utils service database drbd enable-ha
Stopping Heartbeat...
Stopping Mon...
Stopping mon daemon: [ OK ]
Stopping MySQL...
Shutting down MySQL. SUCCESS!
Unmounting DRBD Volume...
Entering DRBD Secondary mode...
Enabling STONITH...
Starting Heartbeat...
[Done]
```

After a few minutes, the HA implementation on the current primary server should automatically turn on the replacement server.

Step 6 Turn on the replacement server if it does not automatically come up within several minutes.

Step 7 Log in to the CLI of the replacement server.

Step 8 Enter **utils service database drbd replace-primary**.

```
admin: utils service database drbd replace-primary
Setting up DRBD Disk
.....
.....
Writing meta data...
initializing activity log
New drbd meta data block successfully created.
Starting DRBD resources: [ d(mysql) s(mysql) n(mysql) ].
Enable Heartbeat...
Starting High-Availability services:
[ OK ]
```

Step 9 Verify that the replacement server currently has the secondary HA role of 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 : 10.22.130.54
The database primary node name : ctx-db-1
The database primary node IP address : 10.22.130.49
The database secondary node name : ctx-db-2
The database secondary node IP address : 10.22.130.57
Mon status : Not running (only runs on primary)
MySQL status : Not running (only runs on primary)
Heartbeat status : Running pid 19094
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res cs ro ds p mounted fstype
... sync'ed: 1.2% (45556/46080)M
```

```
0:mysql SyncTarget Secondary/Primary Inconsistent/UpToDate C
-----
```

Step 10 Log in to the CLI of the current primary database server.

Step 11 Enter **utils service database drbd keep-node**.

```
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]
```

The database servers will automatically begin the synchronization process.

What to Do Next

Complete the following procedures:

- [Verifying Synchronization and Network Connectivity of the Database Servers](#), page 5-12
- [Verifying Data Connectivity Among the Servers](#), page 5-22

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 Make sure 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. To simplify management, Cisco recommends that you use the same username and password on all Cisco TelePresence Exchange System servers.
- 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 5-13
- [Installing the Cisco TelePresence Exchange System Administration Servers](#), page 5-18

Step 7 Proceed to the [“Verifying Data Connectivity Among the Servers”](#) section on page 5-22.



CHAPTER 34

Logs

Revised June 29, 2011

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 2

Appendixes

- [Installation Worksheets](#)
- [Endpoint Capacity](#)
- [Command Reference](#)
- [MIB Reference](#)



APPENDIX **A**

Installation Worksheets

Revised June 29, 2011

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 4-6.

Table A-1 **Worksheet for Cisco TelePresence Exchange System Servers**

Node	Hostname	IP Address	Subnet Mask	Default Gateway	Administrator Username	Password
Database—shared virtual ¹				—	—	—
Database—primary						
Database—secondary						
Database—primary IMM ²	—					
Database—secondary IMM	—					
Engine 1						
Engine 1—IMM (optional)	—					
Engine 2						
Engine 2—IMM (optional)	—					
Admin 1						
Admin 1—IMM (optional)	—					
Admin 2						
Admin 2—IMM (optional)	—					
Security password to authenticate data requests between the database server and the other servers ³						

1. The virtual hostname and virtual IP (VIP) address are shared by both the primary and secondary database servers.
2. IMM = integrated management module. The IMM configuration is required to provide active/standby redundancy on the database servers. For the call engine and administration servers, you need to configure the IMM only if you want remote control.
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.

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 LSCs¹ 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**

Endpoint Capacity

Revised June 29, 2011

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.

Table B-1 describes the number of segments that the Cisco TelePresence Exchange System reserves for a Meet-Me call given a number of variables.



Note

The minimize capacity functionality is available only in Cisco TelePresence Exchange System Release 1.0(3) and later.

Table B-1 **Endpoint Capacity for Meet-Me Calls**

Type of Call	Endpoint Type	Number of Screens	Bridge Type	Number of Segments Reserved Without Minimize Capacity	Number of Segments Reserved with Minimize Capacity
Reserved dial in	Cisco TelePresence System	1	Cisco TelePresence Multipoint System	4	2
		3		4	4
		Unknown		4	4
	Cisco TelePresence Server MSE 8710	1	3	1	
		3	3	3	
		Unknown	3	3	
Dial out	H.323	1	Cisco TelePresence Server MSE 8710	1	1
		3		3	3
		Unknown		1	1
Guest dial out					
Dial out call		1	Cisco TelePresence MCU MSE 8510	1	1
Guest dial out		Unknown		1	1

Table B-1 *Endpoint Capacity for Meet-Me Calls (continued)*

Type of Call	Endpoint Type	Number of Screens	Bridge Type	Number of Segments Reserved Without Minimize Capacity	Number of Segments Reserved with Minimize Capacity
Dial out	ISDN	1	Cisco TelePresence Server MSE 8710	1	1
Guest dial out		Unknown		1	1
Dial out		1	Cisco TelePresence MCU MSE 8510	1	1
Guest dial out		Unknown		1	1

Please note the following bridge limitations:

- Dial out calls are not supported on Cisco TelePresence System endpoints.
- Guest dial out to three-screen H.323 endpoints is not supported.
- The Cisco TelePresence System endpoints and three-screen H.323 endpoints are not supported on the Cisco TelePresence MCU MSE 8510.



APPENDIX **C**

Command Reference

Revised June 29, 2011

This appendix describes the CLI commands that are supported on the Cisco TelePresence Exchange System:

- [file dump](#), page C-3
- [file get](#), page C-5
- [file list](#), page C-7
- [file search](#), page C-8
- [file tail](#), page C-10
- [file view](#), page C-12
- [set adminserver changedbip](#), page C-14
- [set adminserver trapvip](#), page C-15
- [set cdp disable](#), page C-16
- [set cdp enable](#), page C-17
- [set cdp holdtime](#), page C-19
- [set cdp timer](#), page C-20
- [set network failover dis](#), page C-21
- [set network failover ena](#), page C-23
- [set network gateway](#), page C-24
- [set network ip eth0](#), page C-25
- [set password admin](#), page C-27
- [set sipserver changedbip](#), page C-28
- [set sipserver siplb dis](#), page C-29
- [set sipserver siplb ena](#), page C-30
- [set snmp trapdest add](#), page C-31
- [set snmp trapdest del](#), page C-32
- [set snmp user add](#), page C-34
- [set snmp user del](#), page C-35
- [show cdp](#), page C-36

- [show dbip](#), page C-37
- [show engineip](#), page C-38
- [show network eth0](#), page C-39
- [show network failover](#), page C-41
- [show role](#), page C-43
- [show siplb](#), page C-45
- [show snmp trapdests](#), page C-46
- [show snmp users](#), page C-47
- [show trapvip](#), page C-48
- [utils network ping](#), page C-49
- [utils service adminserver start](#), page C-50
- [utils service adminserver status](#), page C-51
- [utils service adminserver stop](#), page C-52
- [utils service database drbd disable-ha](#), page C-53
- [utils service database drbd discard-node](#), page C-54
- [utils service database drbd enable-ha](#), page C-55
- [utils service database drbd force-discard-node](#), page C-56
- [utils service database drbd force-keep-node](#), page C-57
- [utils service database drbd force-mysql-reset](#), page C-58
- [utils service database drbd keep-node](#), page C-60
- [utils service database drbd replace-primary](#), page C-61
- [utils service database status](#), page C-62
- [utils service database sync](#), page C-64
- [utils service list](#), page C-66
- [utils service sipserver start](#), page C-67
- [utils service sipserver status](#), page C-68
- [utils service sipserver stop](#), page C-69
- [utils service start](#), page C-70
- [utils service stop](#), page C-71
- [utils snmp get](#), page C-72
- [utils snmp hardware-agents restart](#), page C-73
- [utils snmp walk](#), page C-74
- [utils system restart](#), page C-76
- [utils system shutdown](#), page C-77

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.
<i>file-spec</i>	Specifies which file or files to dump onto the screen. You can use an asterisk (*) as a wildcard. Enter the <i>file-spec</i> as one of the following items: <ul style="list-style-type: none"> • Directory • Filename • Directory path and filename
recent	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.
<i>file-spec</i>	Specifies which file or files to get via SFTP. You can use an asterisk (*) as a wildcard. Enter the <i>file-spec</i> as one of the following items: <ul style="list-style-type: none"> • Directory • Filename • Directory path and filename
reltime	Gets files that are no older than the specified <i>reltime-age</i> .
<i>reltime-age</i>	How recently files must have been updated in order to include them in the get operation. Enter the <i>reltime-age</i> as follows, where you specify the units and then the value: <p>{ months weeks days hours minutes } <i>number</i></p>
abstime	Gets files that have been updated between the absolute times <i>abstime-start</i> and <i>abstime-end</i> .
<i>abstime-start</i> <i>abstime-end</i>	Enter the <i>abstime-start</i> and the <i>abstime-end</i> as <i>hh:mm:MMIDDIYY</i> , to specify the hour, minute, month, day, and year.
match	Gets files whose filenames contain characters that match a regular expression.
<i>regex</i>	Regular expression for which you want to find matches in the filenames.
recurs	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.
<i>file-spec</i>		Directory whose files and subdirectories you want to list. You can use an asterisk (*) as a wildcard.
page		Displays the output one screen at a time.
detail		Includes the details of each file and subdirectory in the list.
reverse		Displays the list in the reverse sort order.
date		Sorts the list items by date.
size		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 [retime retime-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.
<i>file-spec</i>	Specifies which directories or files to search. You can use an asterisk (*) as a wildcard. Enter the <i>file-spec</i> as one of the following items: <ul style="list-style-type: none"> • Directory • Filename • Directory path and filename
<i>reg-exp</i>	Regular expression against which you want to find matches in the content of the file or files.
retime	Gets files that are no older than the specified <i>retime-age</i> .
<i>retime-age</i>	How recently files must have been updated in order to include them in the get operation. Enter the <i>retime-age</i> as follows, where you specify the units and then the value: <p>{days hours minutes} number</p>
abstime	Searches files that have been created or updated between the absolute times <i>abstime-start</i> and <i>abstime-date</i> .
<i>abstime-start</i> <i>abstime-end</i>	Enter the <i>abstime-start</i> and <i>abstime-date</i> as <i>hh:mm:ss MM/DD/YY</i> , to specify the hour, minute, second, month, day, and year.
recurs	Search 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.
<i>file-spec</i>	Specifies which 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 <i>file-spec</i> as one of the following items: <ul style="list-style-type: none"> • Filename • Directory path and filename • Directory—If you enter only a directory, you need to specify the file by adding the recent keyword.
<i>num-lines</i>	Number of lines to display in the output. Default: 10.
recent	Specifies the most recently changed file in the directory.

Usage Guidelines

This command is useful 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] -
cuvvmResourceList :[]
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.
<i>file-spec</i>	Specifies which file to view. You can use an asterisk (*) as a wildcard as long as it resolves to a single file. Enter the <i>file-spec</i> 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, use the following command.

```
set adminserver changedbip database-vip-address
```

Syntax Description

<i>database-vip-address</i>	VIP address of the database servers.
-----------------------------	--------------------------------------

Usage Guidelines

Enter 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, use the following command.

```
set adminserver trapvip {ena vip-address | dis}
```

Syntax Description	ena	Description
	<i>vip-address</i>	Adds the VIP address to product-specific notifications. 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

Enter 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

<i>interface</i>	Specifies the 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		
	<i>interface</i>	Specifies the 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 of 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	<i>seconds</i>	Specifies the 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	<i>seconds</i>	Specifies how often, in seconds, the server sends CDP update packets. Default: 60.
--------------------	----------------	---

Usage Guidelines

Make sure 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, use 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, use 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 reenble 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, use the following command.

```
set network gateway ip-address
```

Syntax Description

<i>ip-address</i>	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
      *** WARNING ***
      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, use the following command.

```
set network ip eth0 ip-address subnet-mask
```

Syntax Description

<i>ip-address</i>	IP address of the server.
<i>subnet-mask</i>	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, use 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.

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, use the following command.

```
set sipserver changedbip database-vip-address
```

Syntax Description

<i>database-vip-address</i>	VIP address of the database servers.
-----------------------------	--------------------------------------

Usage Guidelines

Enter 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, use the following command.

```
set sipserver siplb dis
```

SyntaxDescription This command has no arguments or keywords.

Usage Guidelines Enter 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), use the following command.

```
set sipserver siplb ena load-balancer-vip-address [port]
```

Syntax Description

<i>load-balancer-vip-address</i>	VIP address of the SIP load balancer.
<i>port</i>	(Optional) Port number on which the call engine connects to the SIP load balancer. Default: 5060.

Usage Guidelines

Enter 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, use 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		SNMP version 3.
<i>username</i>		SNMP username.
2c		SNMP version 2c.
<i>community-string</i>		Community string.
<i>destination</i>		IP address or hostname of the host to which the system sends the trap notifications.
<i>port</i>		(Optional) Port number. Default: 162.
<i>level</i>		(Optional) Enter one of the following values: <ul style="list-style-type: none"> • 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.
<i>passphrase</i>		(Optional for SNMP version 2c) User password.
<i>engineID</i>		(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, use the following command.

```
set snmp trapdest del
```

Syntax Description This command has no arguments or keywords.

Usage Guidelines When you enter the 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 In the following example, 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, use 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	SNMP version 3.
<i>snmp-username</i>	SNMP username.
2c	SNMP version 2c.
<i>community-string</i>	Community string.
<i>access</i>	Enter one of the following values: <ul style="list-style-type: none"> • r—Read access. • w—Write access. • rw—Read and write access.
<i>level</i>	(Optional for SNMP version 2c) Enter one of the following values: <ul style="list-style-type: none"> • 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.
<i>passphrase</i>	(Optional for noauthNoPriv level or SNMP version 2c) User password.

Usage Guidelines

If you use both SNMP versions 3 and 2c, make sure 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, use 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	SNMP version 3.
<i>snmp-username</i>	SNMP username.
2c	SNMP version 2c.
<i>community-string</i>	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

Enter 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

```
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

Enter 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

Disk/active      Total          Free          Used
Disk/inactive   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
```

show role

	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, use the following command.

```
show siplb
```

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Enter 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, use 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, use 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, use the following command.

```
show trapvip
```

Syntax Description This command has no arguments or keywords.

Usage Guidelines Enter 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	<i>ip-address</i>	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	<pre>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</pre>
-----------------	---

Related Commands	None.
-------------------------	-------

utils service adminserver start

To start an administration server after you a 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

Example on an administration server that is up and running:

```
admin: utils service adminserver status
adminserver.....Not running
```

Example on an administration server that 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 this 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 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 only if the current primary database server fails in such a way that its integrated management module (IMM) becomes unavailable and prevents the current secondary database server from automatically taking over the primary HA role. For details, see the [“Recovering from a Failed Primary Database Server”](#) 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
Stopping Heartbeat...
Disabling STONITH...
[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 because the acting primary server had failed in such a way that its integrated management module (IMM) became unavailable. For details, see the [“Recovering from a Failed Primary Database Server”](#) 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
Stopping Heartbeat...
Stopping Mon...
Stopping mon daemon: [ OK ]
Stopping MySQL...
Shutting down MySQL. SUCCESS!
Unmounting DRBD Volume...
Entering DRBD Secondary mode...
Enabling STONITH...
Starting Heartbeat...
[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 30-7. 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 30-7](#). 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 Failed Primary Database Server, 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 drbd replace-primary

To enable a replacement database server that is installed with the initial primary high-availability (HA) role to instead act in the secondary HA role, enter the following command.

```
utils service database drbd replace-primary
```

Syntax Description This command has no arguments or keywords.

Usage Guidelines Use this command as part of the process to replace a failed database server that was installed with the initial primary HA role. For details, see the [“Recovering from a Failed Primary Database Server”](#) section on page 33-1.

Examples The following example shows how to enable a replacement database server that is installed with the initial primary HA role to instead act in the secondary HA role:

```
admin: utils service database drbd replace-primary
Setting up DRBD Disk
.....
.....
Writing meta data...
initializing activity log
New drbd meta data block successfully created.
Starting DRBD resources: [ d(mysql) s(mysql) n(mysql) ].
Enable Heartbeat...
Starting High-Availability services:
[ OK ]
```

Related Commands	Command	Description
	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:

- Heartbeat is running.
- Connection state (cs) is “Connected.”
A connection state 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 (ro) values indicate that one server has the primary role, and the other server has the secondary role, specifically:
 - The ro state on the left shows the HA role of the server on which you are viewing the command output.
 - The ro state on the right shows the HA role of the redundant peer.
- The disk state (ds) is UpToDate for both servers, specifically:
 - The ds state on the left shows the disk state of the server on which you are viewing the command output.
 - The ds state on the right shows the disk state of the redundant peer.
- MySQL is running (current primary database server only).

During the initial synchronization, the command output indicates the progress of the synchronization process. See the [“Synchronizing the Database Servers” section on page 5-10](#).

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                        : 10.22.130.54
The database primary node name                  : ctx-db-1
The database primary node IP address            : 10.22.130.49
The database secondary node name                : ctx-db-2
The database secondary node IP address          : 10.22.130.57
Mon status                                      : Running pid 10183
MySQL status                                 : Running pid 10100
Heartbeat status                             : Running pid 20414
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res  cs          ro          ds          p mounted  fstype
0:mysql Connected Primary/Secondary UpToDate/UpToDate C /mnt/mysql ext3
-----
```

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
The database primary node name                  : ctx-db-1
The database primary node IP address            : 10.22.130.49
The database secondary node name                : ctx-db-2
The database secondary node IP address          : 10.22.130.57
Mon status                                      : Not running (only runs on primary)
MySQL status                                    : Not running (only runs on primary)
Heartbeat status                             : Running pid 17842
-----
drbd driver loaded OK; device status:
version: 8.3.2 (api:88/proto:86-90)
m:res  cs          ro          ds          p mounted  fstype
0:mysql Connected Secondary/Primary UpToDate/UpToDate C
-----
```

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 database sync

To synchronize the primary and secondary database servers, enter the following command.

```
utils service database sync
```

Syntax Description This command has no arguments or keywords.

Usage Guidelines See the [“Synchronizing the Database Servers”](#) section on page 5-10.

Examples In the following example, the command is entered after the database servers have already been synchronized:

```
admin: utils service database sync
-----
DRBD is already running..no need to sync data
-----
```

The following example shows how to initiate the synchronization process on the initial primary database server:

```
admin: utils service database sync
Setting up DRBD Disk
.....
.....
Writing meta data...
initializing activity log
New drbd meta data block successfully created.
Starting DRBD resources: [ d(mysql) s(mysql) n(mysql) ]
.
Setting up Primary node...
Creating filesystem for MySQL HA...
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 31 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.
Moving MySQL to HA DRBD...
```



```

Enable Heartbeat...
Starting High-Availability services:
[ OK ]
Starting Data sync procedures.....
Please wait...Database access can take upto 2 minutes.

```

The following example shows how to initiate the synchronization process on the initial secondary database server:

```

admin: utils service database sync
Setting up DRBD Disk
.....
.....
Writing meta data...
initializing activity log
New drbd meta data block successfully created.
Starting DRBD resources: [ d(mysql) s(mysql) n(mysql) ].
Setting up Secondary node...
Enable Heartbeat...
Starting High-Availability services:
[ OK ]

```

Related Commands

Command	Description
utils service database status	Checks the status of a database server.

utils service list

To display which services have and have not started, enter the following command.

utils service list

Syntax Description This command has no arguments or keywords.

Usage Guidelines Use this command to check the status of services on any Cisco TelePresence Exchange System server.

Examples The following example shows that all services have started:

```
admin: utils service list

Requesting service status, please wait...
System SSH [STARTED]
Cluster Manager [STARTED]
SNMP [STARTED]
```

Related Commands

Command	Description
utils service start	Starts a service.
utils service stop	Gracefully stops a service.

utils service sipserver start

To 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 Example on a call engine server that is up and running:

```
admin: utils service sipserver status
sipserver.....<Pid: 3223> running
```

Example on a call engine server that was 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 this 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 service start

To start a service, enter this command.

```
utils service start service
```

Syntax Description

<i>service</i>	Name of the service.
----------------	----------------------

Usage Guidelines

This command is case-sensitive and accepts only the service names that are displayed in the CLI output of the **utils service list** command.

Examples

The following example shows how to view the status of each service and to start one that has not yet started:

```
admin: utils service list

Requesting service status, please wait...
System SSH [STARTED]
Cluster Manager [STARTED]
SNMP [STOPPED] Service Not Started

admin: utils service start SNMP
Service Started
SNMP [STARTED]
```

Related Commands

Command	Description
utils service list	Displays whether or not each service has started.
utils service stop	Gracefully stops a service.

utils service stop

To gracefully stop a service, enter this command.

```
utils service stop service
```

Syntax Description	<i>service</i>	Name of the service.
--------------------	----------------	----------------------

Usage Guidelines This command is case-sensitive and accepts only the service names that are displayed in the CLI output of the **utils service list** command..

Examples The following example shows how to view the status of each service and to stop one:

```
admin: utils service list

Requesting service status, please wait...
System SSH [STARTED]
Cluster Manager [STARTED]
SNMP [STARTED]

admin: utils service stop SNMP
Service Stopped
SNMP [STOPPED]

admin: utils service list

Requesting service status, please wait...
System SSH [STARTED]
Cluster Manager [STARTED]
SNMP [STOPPED] Service Not Started
```

Related Commands	Command	Description
	utils service list	Displays whether or not each service has started.
	utils service start	Starts a service.

utils snmp get

To get the SNMP data for a discrete MIB object, use 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	SNMP version 3.
<i>username</i>	SNMP username.
2c	SNMP version 2c.
<i>community-string</i>	Community string.
<i>ip-address</i>	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.
<i>object-id</i>	Object ID (OID).
<i>file</i>	(Optional) Filename or directory path to the file for the output.

Usage Guidelines

The **utils snmp get** 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, use 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, use 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	SNMP version 3.
	<i>username</i>	SNMP username.
	2c	SNMP version 2c.
	<i>community-string</i>	Community string.
	<i>ip-address</i>	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.
	<i>object-id</i>	Object ID (OID).
	<i>file</i>	<i>Not supported.</i>

Usage Guidelines

The **utils snmp walk** 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 this 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 This command is used 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

Revised June 29, 2011

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:

- [Update Intervals for SNMP Tables, page D-1](#)
- [Overall Health System Status Objects, page D-2](#)
- [Table Objects, page D-3](#)
- [Trap Notification Objects, page D-5](#)
- [Read-Write Objects, page D-8](#)

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	<i>Not supported.</i>
	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 an 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: <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Default is true (enabled).</p> <p>This object controls the generation of the following notifications:</p> <ul style="list-style-type: none"> • ciscoCTXSysAdminServersStatusChg • ciscoCTXSysDatabaseServersStatusChg • ciscoCTXSysCallEnginesStatusChg • ciscoCTXSysResourceStatusChg • ciscoCTXSysSystemConfigStatusChg • ciscoCTXSysSystemBackupStatusChg
ctxLicenseAlarmNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.2	<p>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.</p> <p>Default is true (enabled).</p> <p>This object controls the generation of the notification ciscoCTXSysLicenseFailure.</p>
ctxAuthFailureNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.3	<p>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.</p> <p>The default setting for authentication failures is false (disabled) in order to prevent unnecessary event flooding.</p> <p>This object controls the generation of the notification ciscoCTXSysUserAuthFailure.</p>
ctxClusterNodeAlarmNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.4	<p>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.</p> <p>Default is true (enabled).</p> <p>This object controls the generation of the following notifications:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Default is true (enabled).</p> <p>This object controls the generation of the following notifications:</p> <ul style="list-style-type: none"> • ciscoCTXSysResourceDown • ciscoCTXSysResourceUp • ciscoCTXSysResourceAllocFailure
ctxCallFailureNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.6	<p>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.</p> <p>Default is true (enabled).</p> <p>This object controls the generation of the following notifications:</p> <ul style="list-style-type: none"> • ciscoCTXSysCallSetupFailure • ciscoCTXSysCallAbnormalDisconnect
ctxErrorHistoryEventNotifyEnable	1.3.6.1.4.1.9.9.758.1.5.2.7	<p>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.</p> <p>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.</p> <p>Use ctxErrorHistoryMaxSeverity to specify the maximum severity level to be logged and sent via a notification.</p> <p>Default is false (disabled).</p> <p>This object controls the generation of the notification ciscoCTXSysErrorHistoryEvent.</p>
ctxErrorHistoryTableSize	1.3.6.1.4.1.9.9.758.1.4.1	<p>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.</p> <p>A value of '0' disables the history table. The default value is set to 100 entries.</p>

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	<p>Defines the maximum severity of the event messages that the history table will contain.</p> <p>The default is notice(5), which can be changed by setting the object. Available options:</p> <ul style="list-style-type: none"> • 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	<p>This object specifies the number of time intervals that are kept in the history tables ctxPeakHistAllocTable and ctxPeakHistAllocPoolTable.</p> <p>The default is 96 intervals, which at the ctxPeakHistIntTime default of 15 minutes, stores peak values for 24 hours.</p> <p>A value of 0 will disable peak history tables from collecting data.</p> <p>The range is from 5 to 1440 intervals.</p> <p>Changing this value will reset and clear both ctxPeakHistAllocTable and ctxPeakHistAllocPoolTable table entries.</p>
ctxPeakHistIntTime	1.3.6.1.4.1.9.9.758.1.3.4.2	<p>This object specifies the time interval in minutes.</p> <p>The default is 15 minutes.</p> <p>The range is from 1 to 1440 minutes.</p> <p>Changing this value will reset and clear both ctxPeakHistAllocTable and ctxPeakHistAllocPoolTable table entries.</p>

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](#)



GLOSSARY

Revised June 29, 2011

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. <i>See also</i> active/active .
call routing	On the Cisco TelePresence Exchange System, a route is a reference to an adjacency on a Session Border Controller (SBC). Each adjacency on the SBC is assigned a unique tag. The tag value is included in SIP messages between the SBC and Cisco TelePresence Exchange System, which allows simplified routing tables on the SBC.
capacity	The number of segments/ports that are required to include an endpoint in a meeting. The system uses endpoint capacity to reserve and allocate media resources for meetings. The scheduling API provides parameters to reserve extra capacity for a meeting and to specify the capacity for unknown endpoint types. <i>See also</i> segment .
Cisco Aggregation Series Router	Provides SIP session border control for the Cisco TelePresence Exchange System. <i>See also</i> 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. <i>See also</i> 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. One Cisco TelePresence Multipoint Switch provides support for a maximum of 48 table segments. <i>See also</i> segment .
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. <i>See also</i> endpoint .
cluster	<i>See</i> server cluster .
cluster node	One of the nodes in the server cluster. <i>See also</i> server cluster .
common installer	A common installation script that is used to install the Cisco TelePresence Exchange System administration, database, and call engine servers. <i>See also</i> 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. <i>See also</i> active/standby .
direct-dial calls	The Cisco TelePresence Exchange System supports ad hoc and scheduled direct-dial calls between two endpoints in the same organization. The system does not reserve any media resources for direct dialed calls. <i>See also</i> ad hoc meeting and scheduled meeting .

E

endpoint	A Cisco TelePresence endpoint such as a CTS 500. Direct-dial calls are initiated between endpoints. Multipoint meetings are scheduled 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. <i>See also</i> 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. <i>See also</i> 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 conference.

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 a customized Meet-Me service number and greeting to be applied to a Cisco TelePresence call. *See also* [Meet-Me service](#).
- interprovider call** Cisco TelePresence call that is placed between subscribers who are hosted by different service providers.
- Inter-company 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.
- 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.
- 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. <i>See also</i> 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). <i>See also</i> session border controller (SBC) .
Meet-Me service	Rendezvous conference service in which the participants join the meeting by using a pre-arranged meeting ID. The Cisco TelePresence Exchange System provides business-to-business telepresence services.
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. <i>See also</i> 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. <i>See also</i> 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. <i>See also</i> hosted endpoint service and enterprise endpoint service .
organization ports management	An optional feature that 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.

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. Meet-Me and direct dial calls are placed on provisioned endpoints. 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** Endpoint for which no configuration details are known. Remote endpoints are endpoints that join the meeting from another service provider network. Configuring a remote endpoint on the Cisco TelePresence Exchange System reserves capacity for the endpoint on the service provider network on which it resides. The Cisco TelePresence Exchange System automatically determines and reserves the capacity to support these interprovider meetings.
- remote meeting** A remote meeting uses media resources hosted by a remote Cisco TelePresence Exchange System. You schedule a remote meeting to provide One-Button-to-Push (OBTP) functionality to the provisioned endpoints.

S

- scheduled meeting** A meeting that starts at a future time. The meeting host contacts the designated scheduler to reserve the meeting. 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)	<p>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.</p> <p>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.</p>
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.
standing meeting	A meeting that remains active until you delete it.
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. <i>See also</i> 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	<i>See</i> Cisco Unified Communications Manager (Unified CM) .
unprovisioned endpoint	Endpoint for which no configuration details are known by the administrator except the name of the meeting scheduler for that endpoint. You configure an unprovisioned endpoint on the Cisco TelePresence Exchange System to reserve bandwidth for the endpoint on the service provider network. This allows the endpoint to connect with other known endpoints within the network that are scheduled for the same meeting. This capability is useful for intercompany meetings.

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.
-----------------------------	--

