



Troubleshooting Guide for Cisco CallManager

Release 3.3(3)

Corporate Headquarters

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

Customer Order Number: DOC-7815613=
Text Part Number: 78-15613-01



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 NON-INFRINGEMENT 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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0303R)

Troubleshooting Guide for Cisco CallManager

Copyright © 2002-2003 Cisco Systems, Inc.

All rights reserved.



Preface xi

Purpose **xi**

Audience **xii**

Organization **xii**

Related Documentation **xiv**

Conventions **xv**

Obtaining Documentation **xvi**

 Cisco.com **xvi**

 Documentation CD-ROM **xvii**

 Ordering Documentation **xvii**

 Documentation Feedback **xviii**

Obtaining Technical Assistance **xviii**

 Cisco.com **xviii**

 Technical Assistance Center **xix**

Obtaining Additional Publications and Information **xxi**

CHAPTER 1

Troubleshooting Overview 1-1

Cisco CallManager **1-1**

Serviceability **1-2**

Hardware and Software Compatibility **1-3**

General Model of Problem Solving **1-3**

Network Failure Preparation **1-4**

IP Telephony Networks **1-5**

Where to Find More Information **1-5**

CHAPTER 2

Troubleshooting Tools 2-1

Sniffer Traces **2-1**

Debugs **2-2**

Cisco CallManager Troubleshooting Tools **2-3**

 Cisco CallManager Administration Serviceability Tool **2-5**

 Alarms **2-6**

 Traces **2-6**

 Real-Time Monitoring **2-11**

 Service Activation **2-12**

 Control Center **2-13**

 Microsoft Performance Monitor **2-13**

 Microsoft Event Viewer **2-17**

 Cisco Secure Telnet **2-18**

 Command Line Tools **2-18**

 Simple Network Management Protocol Support **2-20**

 CiscoWorks2000 **2-21**

 Other Tools **2-21**

Troubleshooting Tips **2-22**

Where to Find More Information **2-28**

CHAPTER 3

Installation, Backup, and Restore Issues 3-1

Quick Upgrade, Backup, and Restore Tips **3-2**

 Restore Location When You Have Two Different Versions of
 Cisco CallManager **3-2**

 BAT for Faster Transfer of Data **3-2**

 Upgrade, Backup, and Restore **3-2**

 Back Up the Publisher **3-3**

 Third-Party Backup Utilities **3-3**

Installation Issues 3-3

Unable to Change the Server Name for Cisco CallManager **3-4**

Boot Failure Recovery **3-4**

One Publisher, Two Subscribers: All Three Databases Have Different Information After an Install on One Subscriber **3-5**

Upgrade Issues 3-6

BIOS Upgrade for the MCS-7830 **3-6**

Browser Service: Every 2 Hours, an Error Occurs in the Event Log on the Subscriber **3-7**

Blank Enterprise Parameters Page After Upgrade **3-8**

Related Information **3-9**

Backup and Restore Issues 3-9

Backup to Local Tape Drive Is Not Working and Terminates with Error Code 1165 **3-11**

Unable to Cancel the "Cancelling Backup Process. Please wait..." Message **3-11**

When Installing Cisco CallManager, No Prompt Displays for a Backup Destination **3-12**

Related Information **3-13**

After a Restore, Database Is Corrupt **3-14**

CHAPTER 4**Cisco CallManager System Issues 4-1**

Cisco CallManager System Not Responding **4-2**

Cisco CallManager System Stops Responding **4-3**

Cisco CallManager Administration Page Does Not Display **4-4**

Errors Occur When Attempting to Access the Cisco CallManager Administration Page from the Browser **4-6**

A Virus is Affecting the Server Performance **4-9**

You Are Not Authorized to View This Page **4-11**

Errors Occur When Attempting to Access the Cisco CallManager Administration Page from a Browser on a Remote Server **4-14**

- Name to Address Resolution Failing **4-14**
- Default Web Site Under IIS Has Improper Setting **4-15**
- Port 80 Is Blocked in One or More Routers Between Your Local Browser and the Cisco CallManager Server **4-16**
- You Attempt to Access a Machine Where Access Is Explicitly Denied **4-17**
- Improper Network Setting Exists in the Remote Machine From Where You Are Browsing **4-18**
- Replication Fails Between the Publisher and the Subscriber **4-20**
- Slow Server Response **4-21**
- Security **4-22**
 - Changing IIS Parameters for Security **4-22**
 - Near-Term Security Solutions **4-23**
 - Long-Term Security Solutions **4-23**
 - Related Information **4-24**
- Virus Protection **4-24**
 - Code Red II Recovery **4-25**

CHAPTER 5**Directory Issues 5-1**

- DC Directory Stability **5-2**
 - Resolving Replication Problems Between DC Directory Servers in a Cisco CallManager Cluster **5-5**
 - Application Profiles Are Not Shown for User Configuration with the DC Directory **5-8**
 - Users List Is Not Visible from the Cisco CallManager Administration or Basic User Search Returns Nothing **5-10**
 - Add a New User Does Not Work and You Cannot Access the DC Directory Administrator **5-11**
- Related Information **5-15**

CHAPTER 6**Device Issues 6-1**Voice Quality **6-2**Lost or Distorted Audio **6-2**Correcting Audio Problems from the Cisco IP Phone **6-5**Echo **6-7**One-Way Audio or No Audio **6-9**Codec and Region Mismatches **6-11**Location and Bandwidth **6-12**Phone Resets **6-12**Dropped Calls **6-13**Gateway Reorder Tone **6-15**Gateway Registration Failure **6-16**Gatekeeper Issues **6-23**Intercluster Trunks or H.225 Trunks **6-24**Admission Rejects **6-24**Registration Rejects **6-25**Cisco CallManager Locks the B-Channel and Sends Restart **6-25**B-Channel Remains Locked When Restart_Ack Does Not Contain
Channel IE **6-29**

CHAPTER 7**Dial Plans and Routing Issues 7-1**Route Partitions and Calling Search Spaces **7-1**Dial Plans **7-4**Secure Dial Plan **7-6**

CHAPTER 8**Cisco CallManager Services Issues 8-1**Conference Bridge Issues **8-1**

Transcoding Issues **8-3**
MTP Resource Issues **8-6**

CHAPTER 9

Voice Messaging Issues 9-1

Voice Messaging **9-1**
 Voice Messaging Stops After 30 Seconds **9-1**
Unity Issues **9-2**
 Unity Does Not Roll Over: Receive Busy Tone **9-3**
 Calls Forwarded to Voice Messaging Are Treated as a Direct Call to Unity **9-3**
 Administrator Account Not Associated with Cisco Unity Subscriber **9-4**
 Noise in Recorded Message on Cisco Unity 3.1.2 or 3.1.3 **9-6**

APPENDIX A

Opening a Case With TAC A-1

Required Preliminary Information **A-1**
 Network Layout **A-2**
 Problem Description **A-3**
 General Information **A-3**
TAC Web **A-4**
CCO Cases **A-4**
Attachments **A-4**
Cisco Live! **A-5**
Remote Access **A-5**
Cisco Secure Telnet Structure **A-6**
Firewall Protection **A-6**
Cisco Secure Telnet Design **A-6**
Cisco Secure Telnet Structure **A-7**
Where to Find More Information **A-8**

APPENDIX B**Case Study: Troubleshooting Intracluster Phone Calls B-1**Sample Topology **B-2**Cisco IP Phone Initialization Process **B-3**Skinny Station Registration Process **B-4**Cisco IP Phone-to-Cisco IP Phone Call Flow Within a Cluster **B-7**Cisco IP Phone-to-Cisco IP Phone Exchange of Skinny Station Messages During Call Flow **B-8**Cisco CallManager Initialization Process **B-10**Self-Starting Processes **B-11**Cisco CallManager Registration Process **B-12**Cisco CallManager KeepAlive Process **B-14**Cisco CallManager Intracluster Call Flow Traces **B-15**

APPENDIX C**Case Study: Troubleshooting Cisco IP Phone-to-Cisco IOS Gateway Calls C-1**Call Flow Traces **C-2**Debug Messages and Show Commands on the Cisco IOS Gatekeeper **C-5**Debug Messages and Show Commands on the Cisco IOS Gateway **C-6**Cisco IOS Gateway with T1/PRI Interface **C-11**Cisco IOS Gateway with T1/CAS Interface **C-12**

APPENDIX D**Case Study: Troubleshooting Intercluster Phone Calls D-1**Sample Topology **D-1**Intercluster H.323 Communication **D-1**Call Flow Traces **D-2**Failed Call Flow **D-4**

INDEX



Preface

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

The preface covers these topics:

- Purpose
- Audience
- Organization
- Related Documentation
- Conventions
- Obtaining Documentation
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Purpose

The *Troubleshooting Guide for Cisco CallManager* provides troubleshooting procedures for the Cisco CallManager. This document does not cover every possible trouble event that might occur on a Cisco CallManager system but instead focuses on those events frequently seen by the Cisco Technical Assistance Center (TAC) or frequently asked questions from newsgroups.

Audience

The *Troubleshooting Guide for Cisco CallManager* provides guidance for network administrators responsible for managing the Cisco CallManager system, for enterprise managers, and for employees. This guide requires knowledge of telephony and IP networking technology.

Organization

Table 1 shows how this guide is organized.

Table 1 *How This Document Is Organized*

Chapter and Title	Description
Chapter 1, “Troubleshooting Overview”	Provides an overview of the tools and resources that are available for troubleshooting the Cisco CallManager.
Chapter 2, “Troubleshooting Tools”	Addresses the tools and utilities that you use to configure, monitor, and troubleshoot Cisco CallManager 3.3 and provides general guidelines for collecting information to avoid repetitive testing and recollection of identical data.
Chapter 3, “Installation, Backup, and Restore Issues”	Describes solutions for the most common issues related to a Cisco CallManager installation, backup, or restore.
Chapter 4, “Cisco CallManager System Issues”	Describes solutions for the most common issues related to a Cisco CallManager system.

Table 1 *How This Document Is Organized (continued)*

Chapter and Title	Description
Chapter 5, “Directory Issues”	Describes solutions for the most common issues related to a Cisco CallManager DC Directory (DCD), the Lightweight Directory Access Protocol (LDAP) directory, or the Microsoft Active Directory (AD).
Chapter 6, “Device Issues”	Describes solutions for the most common issues related to IP phones and gateways.
Chapter 7, “Dial Plans and Routing Issues”	Describes solutions for the most common issues related to dial plans, route partitions, and calling search spaces.
Chapter 8, “Cisco CallManager Services Issues”	Describes solutions for the most common issues related to services, such as conference bridges and media termination points.
Chapter 9, “Voice Messaging Issues”	Describes solutions for the most common voice messaging issues.
Appendix A, “Opening a Case With TAC”	Describes what information is needed to open a case for TAC.
Appendix B, “Case Study: Troubleshooting Intracluster Phone Calls”	Describes in detail the call flow between two Cisco IP Phones within a cluster.
Appendix C, “Case Study: Troubleshooting Cisco IP Phone-to-Cisco IOS Gateway Calls”	Describes a Cisco IP Phone calling through a Cisco IOS Gateway to a phone connected through a local PBX or on the Public Switched Telephone Network (PSTN).
Appendix D, “Case Study: Troubleshooting Intercluster Phone Calls”	Describes a Cisco IP Phone calling another Cisco IP Phone located in a different cluster.

Related Documentation

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

- *Cisco CallManager Administration Guide*
- *Cisco CallManager System Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Features & Services Guide*
- *Cisco CallManager Quick Start Guide*
- *Cisco CallManager Installation Instructions*
- *Cisco CallManager Backup and Restore Procedure*
- *Cisco CallManager Attendant Console User Guide*
- *Cisco CallManager Multilevel Administration Access Guide*
- *Cisco CallManager Directory Services Guide*
- *Release Notes for Cisco CallManager Release 3.3(2)*
- *Cisco CallManager Documentation Guide for Release 3.3(2)*
- *Hardware Configuration Guide for the Cisco Voice Gateway 200*
- *Software Configuration Guide for the Cisco Voice Gateway 200*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- *Bulk Administration Tool Guide for Cisco CallManager*
- *Cisco Technical Solution Series: IP Telephony Solution Guide*
- *Guide to Cisco Systems VOIP Infrastructure Solution for SIP*

Conventions

This document uses the following conventions:

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

Notes use the following conventions:



Note

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

Timesavers use the following conventions:



Timesaver

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

Tips use the following conventions:



Tips

Means *the information contains useful tips*.

Cautions use the following conventions:



Caution

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

Warnings use the following conventions:



Warning

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

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

<http://www.cisco.com/go/packet>

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

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

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



Troubleshooting Overview

This chapter provides the necessary background information and available resources to troubleshoot the Cisco CallManager.

The chapter covers following topics:

- Cisco CallManager
- Serviceability
- Hardware and Software Compatibility
- General Model of Problem Solving
- Network Failure Preparation
- IP Telephony Networks
- Where to Find More Information

Cisco CallManager

Cisco CallManager provides the software-based, call-processing component of the Cisco IP Telephony Solutions for the Enterprise, part of Cisco AVVID (Architecture for Voice, Video and Integrated Data).

The Cisco CallManager system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services such as unified messaging, multimedia

conferencing, collaborative contact centers, and interactive multimedia response systems interact through Cisco CallManager open telephony application program interface (API).

The Cisco CallManager system includes a suite of integrated voice applications for performing voice conferencing and manual attendant console functions. Because of this suite of voice applications, no need exists for special-purpose, voice-processing hardware.

Supplementary and enhanced services such as hold, transfer, forward, conference, multiple-line appearances, automatic route selection, speed dial, last-number redial, and other features extend to IP phones and gateways. Because Cisco CallManager is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform.

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

Cisco CallManager Administration, a web-based interface to the database, provides remote device and system configuration and serviceability. This interface also provides access to HTML-based online help for users and administrators.

Serviceability

Administrators can use the Cisco CallManager Administration Serviceability Tool (AST) to troubleshoot system problems. AST, a web-based tool, provides the following services:

- Alarms—Saves Cisco CallManager services alarms and events for troubleshooting and provides alarm message definitions.
- Trace—Saves Cisco CallManager services trace information to various log files for troubleshooting. Administrators can configure, collect, and analyze trace information.

- Real-Time Monitoring—Monitors real-time behavior of the components in a Cisco CallManager cluster.
- Control Center—Views status of Cisco CallManager services. Administrators use Control Center to start and stop services.

Access AST from Cisco CallManager Administration by choosing Applications from the menu bar. Installing the Cisco CallManager software automatically installs Serviceability and makes it available.

Refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide* for detailed information and configuration procedures on the serviceability tools.

Hardware and Software Compatibility

Refer to the *Cisco CallManager Compatibility Matrix* document for compatible versions of all Cisco CallManager components.

General Model of Problem Solving

When troubleshooting a telephony or IP network environment, define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

The following steps provide guidelines to use in the problem-solving process.

-
- Step 1** Analyze the network problem and create a clear problem statement. Define symptoms and potential causes.
 - Step 2** Gather the facts that you need to help isolate possible causes.
 - Step 3** Consider possible causes based on the facts that you gathered.
 - Step 4** Create an action plan based on those causes. Begin with the most likely problem and devise a plan in which you manipulate only one variable.
 - Step 5** Implement the action plan, performing each step carefully while testing to see whether the symptom disappears.

- Step 6** Analyze the results to determine whether the problem has been resolved. If it has, the process is complete.
- Step 7** If the problem has not been resolved, create an action plan based on the next most probable cause on your list. Return to Step 4 and repeat the process until the problem has been solved.
- Make sure that you undo anything that you changed while implementing your action plan. Remember that you want to change only one variable at a time.
-

**Note**

If you exhaust all the common causes and actions (either those outlined in this document or others that you have identified in your environment), contact Cisco TAC.

Network Failure Preparation

You can always recover more easily from a network failure if you are prepared ahead of time. To determine if you are prepared for a network failure, answer the following questions:

- Do you have an accurate physical and logical map of your internetwork that outlines the physical location of all of the devices on the network and how they are connected as well as a logical map of network addresses, network numbers, and subnetworks?
- Do you have a list of all network protocols that are implemented in your network for each of the protocols implemented and a list of the network numbers, subnetworks, zones, and areas that are associated with them?
- Do you know which protocols are being routed and the correct, up-to-date configuration information for each protocol?
- Do you know which protocols are being bridged? Are there any filters configured in any of these bridges, and do you have a copy of these configurations? Is this applicable to Cisco CallManager?

- Do you know all the points of contact to external networks, including any connections to the Internet? For each external network connection, do you know what routing protocol is being used?
- Has your organization documented normal network behavior and performance, so you can compare current problems with a baseline?

If you can answer yes to these questions, faster recovery from a failure results.

IP Telephony Networks

Refer to the *Cisco Technical Solution Series: IP Telephony Solution Guide* for information on troubleshooting IP telephony networks.

Where to Find More Information

Additional Cisco Documentation

- *Cisco CallManager Administration Guide*
- *Cisco CallManager System Guide*
- *Cisco CallManager Features & Services Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco WebAttendant User Guide*
- *BAT Administration Tool User Guide*
- *Cisco CallManager Quick Start Guide*
- *Cisco CallManager Installation Instructions*
- *Cisco CallManager Backup and Restore Procedure*
- *Cisco CallManager Attendant Console User Guide*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- *Cisco VG248 Analog Phone Gateway Software Configuration Guide*
- *Cisco Conference Connection Administration Guide*
- *Cisco IP Conference Station 7935 Administration Guide*

- *Cisco Technical Solution Series: IP Telephony Solution Guide*
- *Guide to Cisco Systems VOIP Infrastructure Solution for SIP*
- CiscoWorks2000 user documentation at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm>



Troubleshooting Tools

This chapter addresses the tools and utilities that you use to configure, monitor, and troubleshoot Cisco CallManager 3.3 and provides general guidelines for collecting information to avoid repetitive testing and recollection of identical data.



Note

To access some of the URL sites listed in this document, you must be a registered user and you must be logged in.

This chapter contains the following topics:

- Sniffer Traces
- Debugs
- Cisco CallManager Troubleshooting Tools
- Troubleshooting Tips
- Where to Find More Information

Sniffer Traces

Typically, you collect sniffer traces by connecting a laptop or other sniffer-equipped device on a Catalyst port that is configured to span the VLAN or port(s) (CatOS, Cat6K-IOS, XL-IOS) that contains the trouble information. If no free port is available, connect the sniffer-equipped device on a hub that is inserted between the switch and the device.

**Tip**

To help facilitate reading and interpreting the traces by the TAC engineer, Cisco recommends using Sniffer Pro software because it is widely used within the TAC.

Have available the IP/MAC addresses of all equipment that is involved, such as IP phones, gateways, Cisco CallManagers, and so on.

Debugs

The output from **debug** privileged EXEC commands provides diagnostic information concerning a variety of internetworking events relating to protocol status and network activity in general.

Set up your terminal emulator software (such as HyperTerminal), so it can capture the debug output to a file. In HyperTerminal, click **Transfer**; then, click **Capture Text**, and choose the appropriate options.

Before running any IOS voice gateway debugs, make sure that `service timestamps debug datetime msec` is globally configured on the gateway.

**Note**

Avoid collecting debugs in a live environment during operation hours.

Preferably, collect debugs during non-working hours. If debugs must be collected in a live environment, configure `no logging console` and `logging buffered`. To collect the debugs, use `show log`.

Some debugs can be lengthy, so collect them directly on the console port (default `logging console`) or on the buffer (`logging buffer`). Collecting debugs over a Telnet session may have an impact on the device performance, and the result could be incomplete debugs, which requires that you recollect them.

To stop a debug, use the `no debug all` or `undebug all` commands. Verify that the debugs have been turned off by using the command `show debug`.

Cisco CallManager Troubleshooting Tools

Cisco CallManager supports the troubleshooting tools listed in Table 2-1.

Table 2-1 Troubleshooting Tools

Tool Name	What it does	For more information
Cisco CallManager Administration Serviceability Tool	Monitors real-time behavior of the components in a Cisco CallManager cluster. AST monitors device status, system performance, and device discovery.	See Cisco CallManager Administration Serviceability Tool and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Alarms	Provides information about a Cisco CallManager service to a destination that you configure. Also provides definitions of alarms and the recovery procedure.	See Alarms and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Trace	Configures, collects, and analyzes information in log files for Cisco CallManager services.	See Traces and refer to the <i>Cisco CallManager Administration Guide</i> and the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Real-Time Monitoring	Monitors real-time behavior of the components in a Cisco CallManager cluster.	See Real-Time Monitoring and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.

Table 2-1 Troubleshooting Tools (continued)

Tool Name	What it does	For more information
Service Activation	Views activation status of Cisco CallManager services. You can also activate and deactivate services.	See Service Activation and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Control Center	Views status and starts and stops Cisco CallManager services for a particular server or all servers in a cluster.	See Alarms and refer to the <i>Cisco CallManager Administration Guide Release</i> and the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Microsoft Performance Monitor (Perfmon)	Collects and displays system and device statistics for a local or remote Cisco CallManager installation.	See Microsoft Performance Monitor and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> and microsoft.com for detailed information.
Microsoft Event Viewer	Enables you to identify problems at the system level, such as a gateway.	See Microsoft Event Viewer and refer to microsoft.com for detailed information.
Show Command	Displays the contents of the Cisco CallManager configuration database, configuration file, and memory statistics.	See Show Command and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Cisco Secure Telnet	Provides transparent firewall access to Cisco CallManagers servers on the customer site.	See Cisco Secure Telnet and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.

Table 2-1 Troubleshooting Tools (continued)

Tool Name	What it does	For more information
Simple Network Management Protocol (SNMP)	Enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.	See Simple Network Management Protocol Support and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> .
CiscoWorks2000	Manages the remote Cisco CallManager network	See CiscoWorks2000 and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> and the CiscoWorks2000 documentation for detailed information.
Other tools, such as the Dick Tracy utility	The Dick Tracy utility provides additional information that is not available using the Show command.	See Other Tools and refer to http://www-tac/Teams/AVVID/sj/Ttools/ttools.htm for detailed information.

Cisco CallManager Administration Serviceability Tool

The Cisco CallManager Administration Serviceability Tool (AST), a web-based tool available with the Cisco CallManager Serviceability program, monitors real-time behavior of the components in a Cisco CallManager cluster. The AST uses HTTP and TCP to monitor device status, system performance, and device discovery.

Refer to the *Cisco CallManager Serviceability Administration Guide* for more information on the AST.

Alarms

Alarms, a web-based tool available with the Cisco CallManager Serviceability program, provides two functions:

- Configure alarms and events
- Provide alarm message definitions.

Alarms contain information such as explanation and recommended action. Alarm information includes application name, machine name, and cluster name to help you perform troubleshooting for problems that are not on your local Cisco CallManager.

Refer to the *Cisco CallManager Serviceability Administration Guide* for configuration procedures to view definitions and alarm information.

Traces

The Trace and Alarm tools work together as follows:

- You configure trace and alarm settings for Cisco CallManager services.
- You can direct alarms to the Win2000 event viewer, CiscoWorks2000 Syslog, SDI or SDL trace log files, or to all destinations.
- You can base traces for Cisco CallManager services on debug levels, specific trace fields, and Cisco CallManager devices such as phones or gateways.
- You can perform a trace on the alarms that are sent to the SDI or SDL trace log files.

For IP telephony issues, Cisco CallManager traces prove very important in the troubleshooting process. A TAC engineer may ask you to capture traces to troubleshoot the problem.

This section contains information for the following trace items:

- Trace Configuration
- Trace Collection
- Trace Analysis
- Q931 Translator

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Trace Configuration

You can configure the following Cisco CallManager services for Trace Configuration and to specify the parameters that you want to trace.

- Cisco CallManager
- Cisco Extended Functions
- Cisco CDR Insert
- Cisco CTIManager
- Cisco Database Layer Monitor
- Cisco IP Voice Media Streaming Application
- Cisco Messaging Interface
- Cisco MOH Audio Translator
- Cisco RIS Data Collector
- Cisco Telephony Call Dispatcher
- Cisco TFTP

Use the Trace Configuration tool to specify the parameters that you want to trace for troubleshooting Cisco CallManager problems. The Trace Configuration window provides two types of settings: trace filter and trace output.

Specify the following trace parameters:

- Cisco CallManager server (within the cluster)
- Cisco CallManager service on the server
- Debug level
- Specific trace fields
- Output settings

If the service is a call-processing application such as Cisco CallManager or Cisco CTIManager, you can configure a trace on devices such as phones and gateways; for example, you can narrow the trace to all enabled phones with a directory number beginning with 555.

**Note**

To log alarms in the SDI trace log file, check two check boxes in Trace configuration and one check box in Alarm configuration: the Trace on check box in Trace configuration, the Enable trace file log check box in Trace configuration, and the SDI alarm destination check box in Alarm configuration.

Trace Collection

Use the Trace Collection tool to collect trace information for any Cisco CallManager service, the time and date of the trace for that service, and the trace type (SDI or SDL) for that service. Trace Collection takes the information that you chose and writes it into a single file. You can display the collected results or download them to a file, which you use to troubleshoot the system.

Use the following procedure to collect Cisco CallManager traces and SDL traces.

Procedure

- Step 1** From the Cisco CallManager Administration window, choose **Application > Cisco CallManager Serviceability**.
The Cisco CallManager Serviceability window displays.
- Step 2** Choose **Trace > Configuration** as shown in Figure 2-1.

Figure 2-1 Cisco CallManager Serviceability Window



- Step 3** Choose Cisco CallManager from the Configured Services menu.
- Step 4** In the SDL Trace Type Flags parameter value field, enter **0x8000EB15** as shown in Figure 2-2.

Figure 2-2 SDL Trace Type Flags Parameter Value

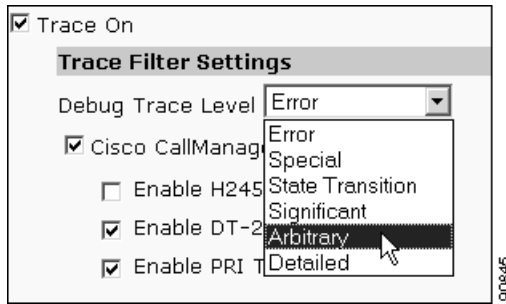
SDL Trace		
Parameter Name	Parameter Value	Suggested Value
SDL Trace Data Flags*	<input type="text" value="0x00000110"/>	0x00000110
SDL Trace Flush Immediately*	<input type="text" value="True"/>	True
SDL Trace Data Size*	<input type="text" value="100"/>	100
SDL Trace Flag*	<input type="text" value="True"/>	True
Sdl TraceType Flags*	<input type="text" value="0x8000EB15"/>	0x8000EB15
Sdl Xml Trace Flag*	<input type="text" value="False"/>	False

Some parameters in this group are hidden, click on Advanced button to see hidden parameters

- Step 5** Check the **Trace On** check box to set CCM and SDL traces to On.

Step 6 Choose **Arbitrary** to set CCM trace setting as shown in Figure 2-3.

Figure 2-3 Trace Filter Settings



Step 7 Click **Update**.

After configuring trace parameters and running the trace, you can choose trace information to collect for analysis. You can base the collection of information on SDL or SDI trace, type of Cisco CallManager service, and time and date of trace. Trace Collection focuses on traces for a specific period.

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Trace Analysis

The Trace Analysis tool, a post-processing tool that displays XML files, provides greater trace detail to help narrow system problems.

Cisco CallManager traces are located at

C:\program files\cisco\traces\ccm

SDL traces are located at

C:\program files\cisco\traces\sdl\ccm

Using the Trace Analysis tool, you can specify an SDI or SDL trace, a device name, or an IP address for the following Cisco CallManager services:

- Cisco CallManager

- Cisco CTIManager
- Cisco TFTP

The system traces the signal distribution layer of the call and logs state transitions into a log file.

Q931 Translator

Use Q931 Translator to translate ISDN/Q931 messages in the SDI trace files to IOS message format. Q931 Translator supports the following formats:

- XML trace file
- Text trace file

You can save the translated trace files to any destination on the network.

Using the message translator tool, Cisco Support Engineers translate your incoming debugging information into familiar Cisco IOS-equivalent messages.

The message translator works by filtering incoming data from Cisco CallManager SDI log files, then parsing and translating them into Cisco IOS-equivalent messages. Message translator supports XML and text files.

Real-Time Monitoring

Cisco CallManager Serviceability provides a web-based tool, Real-Time Monitoring Tool (RTMT), that monitors real-time behavior of the components in a Cisco CallManager cluster. RTMT uses HTTP and TCP to monitor device status, system performance, device discovery, and CTI applications. It also connects directly to devices by using HTTP for troubleshooting system problems.

Performance monitoring provides the following services:

- Monitors performance counters from the Cisco CallManager cluster, including Cisco CallManager nodes, TFTP servers, and database servers.
- Presents counters hierarchically for easy navigation.
- Associates counter threshold settings to alert notification. An email or popup message provides notification to the administrator.

- Permits saving and restoring settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Displays up to three counters in one chart for performance comparisons.

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Service Activation

Cisco CallManager Serviceability provides a web-based Service Activation tool that is used to activate or deactivate multiple services and to choose default services to activate.

Activate or deactivate services in the Service Activate web pages by checking the check boxes beside the service names and clicking the **Update** button.

The Service Activation tool activates services in automatic mode and checks for service dependencies. When you click the **Set Default** button, the Service Activation tool chooses those services that are required to run Cisco CallManager. For example, if you choose one service, all the other services that depend on that service to run Cisco CallManager, if any, also automatically get chosen.



Caution

Only deactivate services from the Service Activation pages. If you deactivate services from the Service Control Manager on the Cisco CallManager system, you will get an error message saying that some of the services are not configured properly. This occurs because deactivating services from the Service Control Manager does not remove the entries from the database tables; therefore, the services get out of sync with the database.



Note

Access the Control Center web pages from a link on the Service Activation pages.

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Control Center

Control Center views status and starts and stops Cisco CallManager services for a particular server or all servers in a cluster. An icon indicates the status of the service. Control Center supports the following Cisco CallManager services:

- Cisco CallManager
- Cisco TFTP
- Cisco Messaging Interface
- Cisco IP Voice Media Streaming Application
- Cisco CTIManager
- Cisco Telephony Call Dispatcher
- Cisco MOH Audio Translator
- Cisco RIS Data Collector
- Cisco Extension Mobility
- Cisco Database Layer Monitor
- Cisco CDR Insert
- Cisco Call Back
- Cisco IP Manager Assistant

Microsoft Performance Monitor

Microsoft Performance Monitor application monitors and logs resource counters from the Cisco CallManager nodes in the network and displays the system activities and status information in real time.

**Tip**

Use the following procedure to collect and display system and device statistics for any Cisco CallManager installation.

Procedure

- Step 1** Access Performance Monitor by choosing **Start > Programs > Administration Tools > Performance**.
- Step 2** Choose **Action > New log settings** and enter a name for the counter log.
- Step 3** Click **Counters**.
- Step 4** Click **Add**.
- Step 5** Click **Performance Object**.
- Step 6** Click **Process**.
- Step 7** In **Select Counters from List** and **Select Instances from List**, choose the following counters and associated instances:
- % Processor Time/_Total
 - % Processor Time/ccm
 - % Processor Time/AudioTranslator
 - % Processor Time/Aupair
 - % Processor Time/CiscoMessagingI
 - % Processor Time/ctftp
 - % Processor Time/CTIManager
 - % Processor Time/DLLHOST
 - % Processor Time/sqlservr
 - % Processor Time/TcdSrv
 - % Processor Time/RisDC
 - % Processor Time/snmp
 - % Processor Time/CallBackService
 - % Processor Time/LogoutService
 - % Processor Time/InsertCDR
 - Virtual Bytes/_Total
 - Virtual Bytes/AudioTranslator
 - Virtual Bytes/Aupair

- Virtual Bytes/ccm
- Virtual Bytes/CiscoMessagingI
- Virtual Bytes/ctftp
- Virtual Bytes/CTIManager
- Virtual Bytes/DLLHOST
- Virtual Bytes/sqlservr
- Virtual Bytes/TcdSrv
- Virtual Bytes/RisDC
- Virtual Bytes/snmp
- Virtual Bytes/CallBackService
- Virtual Bytes/LogoutService
- Virtual Bytes/InsertCDR
- Private Bytes/_Total
- Private Bytes/ccm
- Private Bytes/AudioTranslator
- Private Bytes/Aupair
- Private Bytes/CiscoMessagingI
- Private Bytes/ctftp
- Private Bytes/CTIManager
- Private Bytes/DLLHOST
- Private Bytes/sqlservr
- Private Bytes/TcdSrv
- Private Bytes/RisDC
- Private Bytes/snmp
- Private Bytes/CallBackService
- Private Bytes/LogoutService
- Private Bytes/InsertCDR

- Step 8** Click the **General** tab.
- Step 9** Enter the collection interval of **60** and for Units choose **seconds**, so the data is averaged and collected over 60-second intervals.
- Step 10** Click **Apply**.
- Step 11** Click the **Schedule** tab.
- Step 12** Choose the **At** option for Start log and enter the current time and date to enable the logging to continue after a reboot.
- Step 13** Click **Save** to save your settings, such as the *objects* that you chose.
This allows you to load the same data again, if necessary.

**Note**

The log files will expand in size. Manually purge the log files to maintain optimal disk space.

Performance Monitor can simultaneously collect data from multiple installed systems and store the information in a single log file. You can export the log file into a Tab Separated Value (TSV) file or a Comma Separated Value (CSV) file. View the TSV file or CSV file in a spreadsheet application.

**Note**

You must enable Statistics in Cisco CallManager Administration for the Performance Monitor to collect data.

Cisco CallManager directly updates Microsoft Performance Monitor counters. The call perfmon counters as call-processing-related counters contain simple, useful counts such as number of registered phones, number of active calls, and number of available conference bridge resources.

The following list identifies the Cisco CallManager performance counters:

- Cisco CallManager
- Cisco Phones
- Cisco Lines
- Cisco H323
- Cisco MGCP Gateways

- Cisco MOH Device
- Cisco Analog Access
- Cisco MGCP FXS Device
- Cisco MGCP FXO Device
- Cisco MGCP T1CAS Device
- Cisco MGCP PRI Device

Customize Performance Monitor to view the Cisco CallManager-related parameters that you want to monitor by choosing the object, counter, and the instance.

Refer to microsoft.com for more information on Performance Monitor.

Microsoft Event Viewer

Microsoft Event Viewer tool can help you identify problems at the system level, such as events regarding a specific gateway.

Access Event Viewer by choosing

Start > Programs > Administration Tools > Event Viewer.

The Event Viewer displays the following types of logs:

- Application log—Contains events logged by applications or programs, such as Cisco CallManager.
- System log—Reports events logged by Windows 2000 system components, such as the failure of a component.
- Security log—Holds information records regarding security events. Cisco CallManager does not report events in this log.

The Event Viewer displays the following event types:

- Error—Indicates a problem, such as the loss of data or functionality.
- Warning—Indicates a potential problem, such as when a service is stopped or started. This event type does not necessarily signal an error.
- Information—Indicates the availability of system information, such as host names or the version of the currently used database.

Common Cisco CallManager Event Logs are located at the following URL:
http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/products_tech_note09186a0080111ac2.shtml.

Cisco Secure Telnet

Cisco Secure Telnet allows Cisco Service Engineers (CSE) transparent firewall access to the Cisco CallManager node on your site. Using strong encryption, Cisco Secure Telnet enables a special Telnet client from Cisco Systems to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and troubleshooting of your Cisco CallManager nodes, without requiring firewall modifications.



Note

Cisco provides this service only with your permission. You must ensure that a network administrator is available at your site to help initiate the process.

Command Line Tools

Command Line Tools prove useful in troubleshooting. The following list gives the available command line tools:

- **show**—Displays the Cisco CallManager database content, the .ini config file, memory statistics, and Windows diagnostic information and runs from a DOS shell or from a Telnet session into the Cisco CallManager.
- **nslookup *hostname***—Checks for a host-name-to-IP-address resolution.
- **netstat - a | more**—Checks for socket listens on the correct port number.
- **ping *hostname***—Checks that the machine can be reached via an IP.
- **net start**—Checks to see whether services are running.

Show Command

Use the Show command line tool to display the contents of the system memory statistics and the Windows diagnostic information. You can run the show command from a DOS shell or from a Telnet session if Telnet server software is enabled. You can display the output data on the console or save it as a text file.

**Note**

Because the **show** command uses a temporary file in the \Temp directory for the output, check to see that you have enough disk space available to receive it. The amount that you will need varies depending on a number of factors; for example, the number of users and devices being used and the size of the database being used by the system.

Alternatively, you can run **show.exe** from a Telnet session if Telnet server software is enabled.

The following syntax applies for the show command:

```
show [-f <filename>] [-c <column width>] [-w <console width>] [-v] [command]
```

Table 2-2 lists options that the **show** command supports.

Table 2-2 Show Command Options

Command	Description
-f <filename>	Name of file to print the report
-c <col width>	Width of each column in the database report (default 15)
-w <con width>	Width of the database report area (default 80)
-v	Verbose mode

Use the following parameters with the **show** command:

- **?**—Show help message
- **db**—Show configuration database
- **db tables**—Show database table names
- **db t** <tablename>—Show content of the database table
- **inst** [**apps** | **elem** | **all**]—Show information about installed applications and elements.
- **isdn** [**cluster** | **local** | **specific**]—Show D channel status on gateway.
- **ps**—Show all processes running on the local system.

- **win**—Report windows diagnostics. The **win** command includes, but is not limited to, information such as system statistics, storage information, software environment, and summary statistics.



Note **Show win** consumes a significant part of CPU resources to get the windows system information and takes a long time to display. Execute it only when Cisco CallManager is not busy.

- **tech | (none)**—Report database and Windows system information.



Note **Show tech** reports the same multireport output as **show** command without a parameter

Example:

```
show -f output.txt -v -w480 db
show tech
show db t ProcessNode
```

Refer to the *Cisco CallManager Serviceability Administration Guide* for more information on the **show** command.

Simple Network Management Protocol Support

Network management systems (NMS) use SNMP, an industry-standard interface, to exchange management information between network devices. A part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- A managed device designates a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.
- An agent, as network management software, resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

- A network management system comprises an SNMP management application together with the computer on which it runs. An NMS executes applications that monitor and control managed devices. An NMS provides the bulk of the processing and memory resources that are required for network management. The following NMSs share compatibility with Cisco CallManager:
 - CiscoWorks2000
 - HP OpenView
 - Third-party applications that support SNMP and Cisco CallManager SNMP interfaces

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

CiscoWorks2000

CiscoWorks2000 serves as the network management system of choice for all Cisco devices including Cisco CallManager. Because CiscoWorks2000 is not bundled with Cisco CallManager, you must purchase it separately. Use the following tools with CiscoWorks2000 for remote serviceability:

- System Log
- Path Analysis
- Cisco Discovery Protocol
- Simple Network Management Protocol

Refer to the *Cisco CallManager Serviceability Administration Guide* and the CiscoWorks2000 documentation for more information on CiscoWorks2000 at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm>

Other Tools

Access other available tools, such as the Dick Tracy utility, at the following URL:

<http://www-tac/Teams/AVVID/sj/Ttools/ttools.htm>

Troubleshooting Tips

The following tips may help you when troubleshooting the Cisco CallManager.



Tip

Check the release notes for Cisco CallManager for known problems.

The release notes provide descriptions and workaround solutions for known problems.



Tip

Know where your devices are registered.

Each Cisco CallManager log traces files locally. If a phone or gateway is registered to a particular Cisco CallManager, then the call processing gets done on that Cisco CallManager if the call is initiated there. You will need to capture traces on that Cisco CallManager to debug a problem.

A common mistake involves having devices registered on a subscriber server, but capturing traces on the publisher server. These trace files will be near empty (and most definitely will not have the call in them).

Another common problem involves having Device 1 registered to CM1 and Device 2 registered to CM2. If Device 1 calls Device 2, the call trace occurs in CM1 and if Device 2 calls Device 1 the trace occurs in CM2. If you are troubleshooting a two-way calling issue, you need both traces from both Cisco CallManagers to obtain all the information needed to troubleshoot.



Tip

Know the approximate time of the problem.

Multiple calls may have been made, so knowing the approximate time of the call helps TAC quickly locate the trouble.

You can obtain phone statistics on a Cisco IP Phone 79xx by pressing the **i** button twice during an active call.

When you are running a test to reproduce the issue and produce information, know the following data that is crucial to understanding the issue:

- Calling number/called number
- Any other number that is involved in the specific scenario
- Time of call



Note Remember that time synchronization of all equipment is important for troubleshooting.

If you are reproducing a problem, make sure to choose the file for the timeframe by looking at the modification date and the timestamps in the file. The best way to collect the right trace is to reproduce a problem and then quickly locate the most recent file and copy it from the Cisco CallManager server.



Tip Save the log files to prevent them from being overwritten.

Files will be overwritten after some time. The only way to know which file is being logged to is to choose **View > Refresh** on the menu bar and look at the dates and times on the files.



Tip Verify that the Cisco CallManager services are running.

Use the following procedure to verify that the Cisco CallManager service is active on a server.

Procedure

- Step 1** From Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.
The Cisco CallManager Serviceability window displays.
- Step 2** Choose **Tools > Service Activation** as shown in Figure 2-4.

Figure 2-4 Cisco CallManager Serviceability Window Tools Menu

Step 3 From the Servers column, choose the server.

The server that you chose displays next to the Current Server title, and a box with configured services displays.

Activation Status column displays either Activated or Deactivated in the Cisco CallManager line as shown in Figure 2-5.

Figure 2-5 Service Activation Window

Service Name	Activation Status
NT Service	
<input checked="" type="checkbox"/> Cisco CallManager	Activated
<input checked="" type="checkbox"/> Cisco Tftp	Activated
<input checked="" type="checkbox"/> Cisco Messaging Interface	Activated
<input checked="" type="checkbox"/> Cisco IP Voice Media Streaming App	Activated
<input checked="" type="checkbox"/> Cisco CTIManager	Activated
<input type="checkbox"/> Cisco Telephony Call Dispatcher	Deactivated
<input type="checkbox"/> Cisco MOH Audio Translator	Deactivated
<input checked="" type="checkbox"/> Cisco RIS Data Collector	Activated
<input type="checkbox"/> Cisco Extension Mobility Logout	Deactivated
<input checked="" type="checkbox"/> Cisco Database Layer Monitor	Activated
<input checked="" type="checkbox"/> Cisco CDR Insert	Activated
<input checked="" type="checkbox"/> Cisco Extended Functions	Activated
Tomcat Web Service	
<input checked="" type="checkbox"/> Cisco IP Manager Assistant	Activated

Note: While deactivating a service, make sure to deactivate all of the services that are dependent on this service. Please refer to on-line help for service dependencies for single-server and multi-server configuration.

If Activated, the Cisco CallManager is active on the chosen server.

If Deactivated, continue with the following steps.

Step 4 Check the check box for Cisco CallManager.

Step 5 Click the **Update** button.

The Activation Status column displays Activated in the Cisco CallManager line.

Cisco CallManager is now active for the chosen server.

Perform the following procedure if the Cisco CallManager has been in service and you want to verify if it is currently active.

Procedure

- Step 1** From Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.
The Cisco CallManager Serviceability window displays.
- Step 2** Choose **Tools > Control Center**.
- Step 3** From the Servers column, choose the server.
The server that you chose displays next to the Current Server title, and a box with configured services displays.
Activation Status column displays Activated in the CallManager line.
Cisco CallManager is active for the chosen server.
-



Tip Start and stop the Internet Information Server.

Use either of the following procedures to start or stop the Internet Information Server (IIS).

Procedure

- Step 1** From the Start menu, choose **Start > Programs > Administration Tools > Services**.
A window displays listing the services.
- To Stop Services**
- Step 2** Choose **IIS Admin Service**.
- Step 3** Click the stop button (black square box at the top of the window).
- Step 4** Click **Yes**.

To start Services

- Step 5** Click the **Start** button.
- Step 6** Choose **World Wide Web Publishing**.
- Step 7** Click the start button (black square box with right arrow at the top of the window).
The IIS starts.
-

Procedure

- Step 1** From the Start menu, choose **Start > Programs > Administration Tools > Services**.
A window displays listing the services.

To Stop Services

- Step 2** Right-click **IIS Admin Service**.
- Step 3** Choose **Stop**.
The IIS stops.

To start Services

- Step 4** Click the **Start** button.
- Step 5** Right-click **World Wide Web Publishing**.
- Step 6** Choose **Start**.
The IIS starts.
-

Procedure

- Step 1** From the Start menu, choose **Start > Programs > Administration Tools > Services**.
A window displays listing IIS Administration Service.

- Step 2** Right-click **IIS Admin Service** and choose **Stop**.
The IIS stops.
- Step 3** To start the IIS server:
Right-click **IIS Admin Service** and choose **Start**.
The IIS starts.
-

Where to Find More Information

Additional Cisco Documentation

- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Administration Guide*
- *Installation Guide for Cisco CallManager*
- CiscoWorks2000 user documentation at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm>



Installation, Backup, and Restore Issues

This chapter covers solutions for the following most common issues related to a Cisco CallManager installation, backup, or restore.

- Quick Upgrade, Backup, and Restore Tips
- Installation Issues
- Upgrade Issues
- Backup and Restore Issues

If the following procedures do not solve your problem, contact TAC for a more detailed investigation.

For the latest information to the *Cisco IP Telephony Operating System, SQL Server, Security Updates*, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/osbios.htm

For the *Cisco CallManager Compatibility Matrix*, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

Quick Upgrade, Backup, and Restore Tips

Use the following quick tips to help avoid issues when performing upgrades, backups, and restores to your system:

- Restore Location When You Have Two Different Versions of Cisco CallManager
- BAT for Faster Transfer of Data
- Upgrade, Backup, and Restore
- Back Up the Publisher
- Upgrade Issues

Restore Location When You Have Two Different Versions of Cisco CallManager



Tip

Do a system restore on the same Cisco CallManager version. Changes from release to release cause problems if you try to restore from a different version.

BAT for Faster Transfer of Data



Tip

Build a clean system; then, use the Bulk Administration Tool (BAT) to import your phones and users.

Upgrade, Backup, and Restore



Tip

Perform your upgrade, run the Cisco IP telephony Applications Backup Utility, rebuild the new system from scratch, and restore the backup tape.

Back Up the Publisher

**Tip**

Back up only the publisher server in a Cisco CallManager cluster. All other servers (subscribers) copy over the information on installation.

Third-Party Backup Utilities

For the Unity backup, you need a third-party application.

**Note**

Cisco does not support third-party utilities for backing up the Cisco CallManager database. Doing so voids your TAC support.

**Tip**

Use the included Cisco IP telephony Applications Backup Utility to back up the Cisco CallManager database to a separate machine. Then, use that separate machine to run your third-party backup software.

Installation Issues

For detailed documentation on installation and troubleshooting installs, refer to the *Installation Guide for Cisco CallManager* at the following URL:

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

and click **Installation Instructions** to find the document with the release number for your system software version.

Also refer to the *Release Notes for Cisco CallManager* for any installation issues for your current software version.

This document covers the following installation issues:

- Unable to Change the Server Name for Cisco CallManager
- Boot Failure Recovery
- One Publisher, Two Subscribers: All Three Databases Have Different Information After an Install on One Subscriber

Unable to Change the Server Name for Cisco CallManager

Symptom

You attempt to change the name of the Cisco CallManager server and the service fails. Other services also fail, such as CTI Manager, Extended Functions, and Voice Media Streaming.

Probable Cause

Cisco does not support changing the name of a Cisco CallManager server.

Corrective Action

Change the IP address instead of changing the name of a Cisco CallManager server.

Boot Failure Recovery

The following URL provides detailed Boot Failure recovery procedures:

http://www.cisco.com/warp/public/130/recovery_index.shtml

One Publisher, Two Subscribers: All Three Databases Have Different Information After an Install on One Subscriber

Symptom

Error Message looking for ccmxxxx databases in
(local).master.dbo.sysdatabases table

Probable Cause

The subscriber build failed.

Corrective Action

Procedure

- Step 1** Ensure that the NetBIOS name resolution is working between all servers.
- Step 2** Ensure (by editing) that the hosts and LMHOSTS are filled in on the publisher and subscriber servers, so each one can resolve the other's host name and NetBIOS name.
- Hosts is used for DNS resolution. LMHOSTS uses NetBIOS for name resolution. Also, SQL uses NetBIOS for name resolution.
- Step 3** From the web, upgrade the Cisco CallManager for the software version on your publisher.
- The software will download the SQL database to the subscriber(s).
-

Upgrade Issues

This section covers the following issues for Cisco CallManager upgrades:

- BIOS Upgrade for the MCS-7830
- Browser Service: Every 2 Hours, an Error Occurs in the Event Log on the Subscriber
- Blank Enterprise Parameters Page After Upgrade
- Related Information

BIOS Upgrade for the MCS-7830

Symptom

One of the following actions can occur that alerts you to a BIOS problem:

- The installation stalls.
- When you boot the server, you see a BIOS version prior to 11/08/2000.

Probable Cause

Because the BIOS update is independent from your software upgrade, the possibility exists that it was overlooked during an upgrade.

Corrective Action

Procedure

- Step 1** The latest BIOS date is 11/08/2000. Power off (not a reboot) the server to unlock the flash.
- Step 2** Go to the following URL to upgrade your BIOS:
<http://www.compaq.com/support/files/server/us/download/9343.html>
Follow the installation instructions on that site.

The OS Upgrade CD2 also upgrades the BIOS and Array firmware for you.

Step 3 Access the Array firmware at the following URL:

<http://www.compaq.com/support/files/server/us/download/13161.html>

You only need to create Disk 1 of the four-disk set.

Verification

When you boot the server, confirm that the BIOS date is 11/08/2000.

Browser Service: Every 2 Hours, an Error Occurs in the Event Log on the Subscriber

Symptom

Error Message The browser server has failed to retrieve the backup list too many times on transport \Device\netBT_Tcpip (c96xxx) The backup browser is stopping.

Warning: The browser was unable to retrieve a list of servers from the browser master \\AACCMP1 on the network \Device\netBT_Tcpip (c96xxx) the data is the error code.

Probable Cause

Cause indicates a NIC card problem. You need to upgrade the OS to a newer version.

Corrective Action

Procedure

- Step 1** If you have an MCS-7830 and build the OS with the new 2000.1.2 OS installation, run the OS upgrade version 2000.1.3 to fix the NIC card problem.
- If this is not your problem, verify the following actions:
- Step 2** Ensure that your WINS address is correct.
- Step 3** Ensure that Enable NetBIOS over TCP/IP is chosen.
- Step 4** Ensure that the WINS address is correct on the master browser \\AACCM1.
-

Verification

The error does not occur.

Related Information

For the MCS-7825, the current BIOS version is 9/10/01. For other software- or hardware-related upgrade issues, refer to the documentation on CCO at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/>

The following URL provides MCS-78xx Boot Error Codes:

http://www.cisco.com/warp/public/788/AVVID/mcs_boot.html

Blank Enterprise Parameters Page After Upgrade

Symptom

No field or variable information displays on the Enterprise Parameters page. All other pages display correctly.

Probable Cause

Refer to CSCdv65210—Issues occur where an upgrade was not moving all the information to the database.

Corrective Action

Reinitialize the pages by running

```
C:\Program Files\Cisco\bin\Xmltemp\installxml.vbs
```

Verification

The Enterprise Parameters page displays correctly.

Related Information

For detailed information on upgrading your Cisco CallManager, refer to *Upgrading Cisco CallManager* and locate your release number at the following URL:

http://www.cisco.com/univered/cc/td/doc/product/voice/c_callmg/

Click **Installation Instructions** to find the document for your specific software release.

The following URL provides information that is located on the TAC site:

http://www.cisco.com/warp/public/130/upgrade_index.shtml

Backup and Restore Issues

This section covers the following issues for backups:

- Backup to Local Tape Drive Is Not Working and Terminates with Error Code 1165
- Unable to Cancel the “Cancelling Backup Process. Please wait...” Message
- When Installing Cisco CallManager, No Prompt Displays for a Backup Destination

- Related Information
- After a Restore, Database Is Corrupt

The Cisco IP telephony Applications Backup Utility automatically backs up the following items:

- Cisco CallManager database on SQL Server 7, including the Call Detail Records (CDR) database
- Administrative Reporting Tool (ART) database
- DC Directory, LDAP directory
- Distribution .ini, which contains the publisher and subscriber configuration information
- Database.dat, if present
- HKLM\Software\Cisco Systems, Inc.
- Cisco Customer Response Applications (CRA)

For detailed information on backing up the Cisco CallManager, refer to the *Backing Up and Restoring Cisco CallManager* and locate your release number at the following URL:

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

Click **Installation Instructions** to find the document for your specific software release.

Backup to Local Tape Drive Is Not Working and Terminates with Error Code 1165

Symptom

Error Message 1165 The device has indicated that cleaning is required before further operations are attempted.
ERROR_DEVICE_REQUIRED_CLEANING

Probable Cause

Issues exist with the tape drive or the tape.

Corrective Action

Refer to your hardware documentation for details on cleaning the tape drive, or try using a different, clean tape.

Verification

Backup successfully completes with no errors.

Unable to Cancel the “Cancelling Backup Process. Please wait...” Message

Symptom

When you attempt to cancel the backup process during the Sti Backup Utility, the message “Cancelling backup process. Please Wait...” message does not disappear.

Probable Cause

The backup never executed.

Corrective Action

Rebooting the server will not solve the problem.

Use the following procedure to cancel the backup process.

Step 1 Choose **Start > Run** and enter **regedit**.

Step 2 From the Registry Editor, choose **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco Systems > Backup > Config**.

Use one of the following two solutions to end the Sti Backup Utility.

Solution One

Step 3 Manually change the value of the Config registry key to **0**.

Step 4 Manually stop the StiView.exe process by pressing **Ctrl-Alt-Del** and choosing **Task Manager**.

The Windows Task Manager displays.

Step 5 Click the **Processes** tab.

Step 6 Choose **stiView.exe**.

Step 7 Click **End Process**.

Solution Two

Step 8 From your system directory, choose **C:> WINNT > SYSTEM32**.

Step 9 Double-click the **StiBack.exe** file.

When Installing Cisco CallManager, No Prompt Displays for a Backup Destination

Symptom

You cannot locate the backup folder or the Cisco IP telephony Applications Backup Utility.

Probable Cause

If you are installing Cisco CallManager for the first time, you may have clicked **Cancel** on the backup display. If so, the backup destination was not created.

Corrective Action

Two ways exist for you to install the backup utility into the correct folder:

- Copy the “backup” folder from any other blade, which has installed the Cisco IP telephony Applications Backup Utility, and run the `_stBackSetup.exe` file.
- Run `setup.exe` from the “Backup” folder off of the root directory of the Cisco CallManager CD.

Related Information

The following few Microsoft utilities will help you find out what OS patches apply to your Cisco CallManager.

- `Hfnctk.exe`—Displays programs and service pack that are installed on the box and whether newer patches are available.
- `Serverinfo.exe`—Displays basic information and statistics on the system.
- `Qfecheck.exe`—Displays which HotFixes are installed. This utility does not work for SQL and Internet Explorer HotFixes. `Qfecheck` also spikes the processor during the time it runs. Cisco recommends that you run this utility only in a maintenance window.

To view the HotFixes that apply to Internet Explorer, perform the following steps.

Procedure

Step 1 Open your Internet Explorer and click **Help > About Internet Explorer**.

Step 2 View the Update Versions line.

This line will list the Knowledge Base number for each installed HotFix.

After a Restore, Database Is Corrupt

Symptom

A backup and restore appear to successfully complete on the publisher and subscriber servers. One database is missing information. Each database shows different versions of the software.

Probable Cause

A backup was made of one version, and the restore was to a newer software version.

Corrective Action

You must do a system restore on the same Cisco CallManager version. Changes from release to release would cause problems if you tried to restore from a different version.

Use the following procedures to restore databases.

**Note**

Always perform these procedures from the publisher server. Make sure Cisco NT services and IIS Admin service are stopped.

Backup the SQL Database

Procedure

- Step 1** Choose **Start-Programs > Microsoft SQL Server 7.0 or 2000** for Cisco CallManager version 3.3.
- Step 2** Click **Enterprise Manager**.
- Step 3** Double-click **Microsoft SQL Servers**.
- Step 4** Double-click **SQL Server Group**.
- Step 5** Double-click the machine name (the DNS name of the machine).

- Step 6** Double-click **Databases**.
 - Step 7** Click the highest level database beginning with **CCM**.
 - Step 8** Choose **Tools > Backup Database**.
 - Step 9** Choose **Database — complete** and **Overwrite existing media**.
 - Step 10** Click **Add**.
 - Step 11** Enter the type in a file name in the default path.
 - Step 12** Click **OK**.
-

Restore the SQL Database for the Purpose of Viewing the information

Procedure

- Step 1** Ensure you have backed up your database (see the “Backup the SQL Database” procedure).

Unpublish your current database

- Step 2** Ensure that all Cisco NT services and the IIS Admin service are stopped.
- Step 3** Choose **Start > Programs > Microsoft SQL Server 7.0** (or **2000**).
- Step 4** Click **Enterprise Manager**.
- Step 5** Choose **Microsoft SQL Servers > SQL Server Group**.
- Step 6** Click on your *server name*.

For Microsoft SQL 7

- Step 7** Choose **Replicate**.
- Step 8** Choose **Configure Replication**.
- Step 9** Click the **Publication Database** tab in the pop-up window.
- Step 10** Uncheck the name of your currently published database.
- Step 11** Click **OK**.

For Microsoft SQL 2000

- Step 12** Right-click **Server Name > Replication**.
- Step 13** Choose **Configure Publishing > Subscribers > Distribution**.
- Step 14** Click the **Publication Database** tab in the pop-up window.
- Step 15** Uncheck the name of your currently published database.
- Step 16** Click **OK**.

Restore the Customer Database

- Step 17** Ensure that all Cisco NT services and the IIS Admin service are stopped.
- Step 18** Place the customer backup file in **C:MSSQL7BACKUP**.
- Step 19** Choose **Start > Programs > Microsoft SQL Server 7.0 (or 2000)**.
- Step 20** Click **Enterprise Manager**.
- Step 21** Choose **Microsoft SQL Servers > SQL Server Group**.
- Step 22** Double-click **Databases**.
- Step 23** Click the highest numbered database beginning with **CCM**.
- Step 24** Click **Restore Database**.

If you backed up a database and want to restore that database

- Step 25** Choose **first backup to restore**.
 - Step 26** Choose **Database — complete**.
 - Step 27** Click **OK**.
 - Step 28** If you restore a different database to this machine
 - Step 29** Choose **Restore — from device**.
 - Step 30** Click **Select Devices**.
 - Step 31** Click **Add** and enter the filename from which you are restoring.
 - Step 32** Choose **Database — complete**.
 - Step 33** Click **OK**.
 - Step 34** The following message displays:
`Restore of database CCMxxxx completed successfully.`
-

Now you can view the contents of the database by clicking on it in the main window and looking at its tables, users, and other information.

When you are ready to restore your former database, republish it by choosing **Server Name > Replication** and right-click **Configure Publishing > Subscribers > Distribution** and checking your original database.

Restore a Customer Database to Work With Cisco CallManager on Your Machine

Procedure

-
- Step 1** Repeat the previous procedures for unpublishing your database and restoring the Customer Database.
 - Step 2** Delete the following three default users: CiscoCCMUser, CiscoCCMCDR, and CiscoCCMReader by choosing **Tools > SQL Server Query Analyzer**.
 - Step 3** Choose your database from the pull-down menu in the upper right corner of the screen.



Note Choosing the correct database name is important. Otherwise, you risk deleting users from the wrong database.

- Step 4** Enter **Sp_dropuser CiscoCCMUser** and click **Go**.
- Step 5** Click the **Play** button.
- Step 6** The following message displays:
`User CiscoCCMUser successfully removed from database.`
- Step 7** Enter **Sp_dropuser CiscoCCMCDR** and click **Go**.
- Step 8** Click the **Play** button.
- Step 9** The following message displays:
`User CiscoCCMCDR successfully removed from database.`
- Step 10** Enter **Sp_dropuser CiscoCCMReader** and click **Go**.
- Step 11** Click the **Play** button.
- Step 12** The following message displays:
`User Cisco CCMReader successfully removed from database.`

Add the three default users for your machine

- Step 13** Right-click **Users** in the main screen under your database name.
- Step 14** Choose **CiscoCCMUser** and check the "db_owner" box for this user.
- Step 15** Click **OK**.
- Step 16** Choose **CiscoCCMCDR** -and check the "db_owner" box.
- Step 17** Click **OK**.
- Step 18** Choose **CiscoCCMReader** and check the "db_datareader" box.
- Step 19** Click **OK**.

Configuring database tables**ProcessConfig table**

- Step 20** Choose **Tables > ProcessConfig**.
- Step 21** Right-click **ProcessConfig**.
- Step 22** Choose **open > return all rows**.
- Step 23** Click the **SQL** button and Run the following SQL query:

```
SELECT *
FROM ProcessConfig
where
tkservice = 9

ORDER by paramname
choose the exclamation point to run
```

- Step 24** Make note of the paramValue for GlassHouseNodeID
ParamValue for the GlassHouseNodeId in this table matches the fkProcessNode string in the Cisco CallManager and pkid string in ProcessNode.



Note The first set of digits are the least significant.

- Step 25** Change the Server names in all the DBConnection records to match the machine name of your publisher machine.
- Step 26** Change the database names in the DBConnection records to match the current database name.

ProcessNode table

- Step 27** Choose **Tables > ProcessNode**.
- Step 28** Right-click on **ProcessNode** and choose **open > return all rows**.
- Step 29** Change the 'name' column for the publisher (pkid=glassHouseNodeID you previously noted) to be the *ip address* or *machine name* of your machine.

CallManager table

- Step 30** Choose **Tables > CallManager**.
- Step 31** Right-click on **CallManager** and choose **open > return all rows**.
- Step 32** Change the 'processNodeName' column for the CallManager record where fkprocessnode=glassHouseNodeID is correct machine name or the IP address you changed in the ProcessNode table.

Check the registry settings

- Step 33** Open the registry to HKEY_LOCAL_MACHINE > SOFTWARE.
- Step 34** Click **Cisco Systems, Inc.**
- Step 35** Click **DBL**.
- Step 36** Note the value of the DBConnection0 key.
In the value, ensure the value of SERVER is the DNS name of the publisher and that the database version name is correct.

Publish the database

- Step 37** Return to the main tree in Enterprise Manager.
- Step 38** Click on the *server name*.

For Microsoft SQL 7

- Step 39** Choose **Replicate Data**.
- Step 40** Choose **create or manage a publication**.
- Step 41** Choose your *database name*.
- Step 42** Click **Create Publication**.
- Step 43** Choose the name of the database you are restoring and click **Publish**.
A wizard tool displays.
- Step 44** Click **Next**.

- Step 45** Choose **transactional publication**.
- Step 46** Choose **Yes allow immediate updating subscriptions**.
- Step 47** Choose **all subscribers running SQL Server**.
- Step 48** Choose **publish all tables**.
- Step 49** Click **OK**.
- Step 50** Choose **CCMxxxx** as the name of your database.
- Step 51** Choose **no- create without data filters**.
- Step 52** Click **Finish**.

For Microsoft SQL 2000

- Step 53** Choose **New > Publication**.
 - Step 54** Click **Next**.
 - Step 55** Choose your *database name*.
 - Step 56** Click **Next**.
 - Step 57** Choose **Transactional**.
 - Step 58** Click **Next**.
 - Step 59** Click **Next**.
 - Step 60** Choose **publish all tables**.
 - Step 61** Click **Next**.
 - Step 62** Click **Next**.
 - Step 63** Click **Next**.
 - Step 64** Click **Finish**.
-



Cisco CallManager System Issues

This chapter covers solutions for the following most common issues related to a Cisco CallManager system.

- Cisco CallManager System Not Responding
- Replication Fails Between the Publisher and the Subscriber
- Slow Server Response
- Security
- Virus Protection

Cisco CallManager System Not Responding

This document covers the following issues for a Cisco CallManager system not responding:

- Cisco CallManager System Stops Responding
- Cisco CallManager Administration Page Does Not Display
- Errors Occur When Attempting to Access the Cisco CallManager Administration Page from the Browser
- A Virus is Affecting the Server Performance
- You Are Not Authorized to View This Page
- Errors Occur When Attempting to Access the Cisco CallManager Administration Page from a Browser on a Remote Server
- Name to Address Resolution Failing
- Default Web Site Under IIS Has Improper Setting
- Port 80 Is Blocked in One or More Routers Between Your Local Browser and the Cisco CallManager Server
- You Attempt to Access a Machine Where Access Is Explicitly Denied
- Improper Network Setting Exists in the Remote Machine From Where You Are Browsing
- Replication Fails Between the Publisher and the Subscriber

Cisco CallManager System Stops Responding

Symptom

The Cisco CallManager system does not respond.

Probable Cause

Problem may be any of, but not limited to, the following causes:

- Cisco CallManager service stopped.
- The Internet Information Service (IIS) stopped.
- A virus has affected the server.
- The Network Administrator changed the security policy.
- Improper Configuration settings exist.

Corrective Action

Begin troubleshooting the problem locally on the same server where the Cisco CallManager is installed.

If the following procedures do not solve your system problem, contact TAC for a more detailed investigation:

- Cisco CallManager Administration Page Does Not Display
- Errors Occur When Attempting to Access the Cisco CallManager Administration Page from the Browser
- A Virus is Affecting the Server Performance
- You Are Not Authorized to View This Page
- Errors Occur When Attempting to Access the Cisco CallManager Administration Page from a Browser on a Remote Server
- Name to Address Resolution Failing
- Default Web Site Under IIS Has Improper Setting
- Port 80 Is Blocked in One or More Routers Between Your Local Browser and the Cisco CallManager Server

- You Attempt to Access a Machine Where Access Is Explicitly Denied
- Improper Network Setting Exists in the Remote Machine From Where You Are Browsing

Cisco CallManager Administration Page Does Not Display

Symptom

Administration web page does not display.

Probable Cause

The Cisco CallManager service stopped.

Corrective Action

Use the following procedure to verify that the Cisco CallManager service is active on a server that is local or remote.

Procedure

Step 1 From Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.

The Cisco CallManager Serviceability window displays.

Step 2 Choose **Tools > Service Activation**.

Step 3 From the Servers column, choose a server.

The server that you chose displays next to the Current Server title, and a box with configured services displays.

Activation Status column displays either Activated or Deactivated in the Cisco CallManager line.

If Activated, the Cisco CallManager is active on the chosen server and you need to contact TAC for further assistance.

If Deactivated, continue with the following steps.

Step 4 Check the **Cisco CallManager** check box.

Step 5 Click the **Update** button.

The Activation Status column displays Activated in the Cisco CallManager line. Cisco CallManager is now active for the chosen server.

Perform the following procedure if the Cisco CallManager has been in service and you want to check if it is currently active.

Procedure

Step 1 From Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.

The Cisco CallManager Serviceability window displays.

Step 2 Choose **Tools > Control Center**.

Step 3 From the Servers column, choose the server.

The server that you chose displays next to the Current Server title, and a box with configured services displays.

The Activation Status column displays Activated in the Cisco CallManager line.

Cisco CallManager is active for the chosen server. Contact TAC for further assistance.

If Deactivated, continue with the following steps.

Step 4 Check the **Cisco CallManager** check box.

Step 5 Click the **Update** button.

The Activation Status column displays Activated in the Cisco CallManager line. Cisco CallManager is now active for the chosen server.

Verification

Repeat the preceding procedure to verify that the Cisco CallManager service is activated

Errors Occur When Attempting to Access the Cisco CallManager Administration Page from the Browser

Symptom

One of the following error messages displays when you are trying to access the administration page from the same server where the Cisco CallManager resides.

- Internet Explorer—The page cannot be displayed.
- Netscape—Warning box displays: There was no response. The server could be down or is not responding.

Probable Cause

The IIS Admin service or the WWW publishing service does not start automatically as expected. One of these services stopping represents the most frequent reason for the pages not displaying locally.

Corrective Action

Use the following procedure to start the IIS.



Note

If the IIS is stopped, the WWW publishing services may also be stopped. Start the WWW publishing services, which starts the IIS automatically.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

A window displays listing IIS Administration.

Step 2 Right-click **IIS Admin Service**.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The IIS starts.

Start the other services using the following procedure.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

Step 2 Right-click the service.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The service starts.

Verification

Use the following procedure to verify that IIS is started.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

Step 2 Right-click the service.

Step 3 Verify the status, which should display Started.

Step 4 If any service is stopped, perform the following procedures to start the service(s).

Use the following procedure to start the IIS.

**Note**

If the IIS is stopped, WWW publishing services may also be stopped. Start the WWW publishing services, which starts the IIS automatically.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

A window displays listing IIS Admin Service.

Step 2 Right-click **IIS Admin Service**.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The IIS starts.

Start the other services using the following procedure.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

Step 2 Right-click the service.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The service starts.

A Virus is Affecting the Server Performance

Symptom

The symptom changes with every virus. The IIS may stop, which results in web pages not displaying. Strange messages may display. Server performance varies or stops.

Probable Cause

Viruses that have affected Microsoft products in turn have infected the Cisco CallManager server.

Corrective Action

Use the following procedure to ensure that you have the necessary patches to protect the Cisco CallManager and Cisco CallManager Applications Servers.

Procedure

- Step 1** Verify that you have the necessary patches to protect your system.
- Step 2** If you do not have the correct patches, go to the following URLs to see if your system may be infected:
- CERT Advisory CA-2001-23 Continued Threat of the “Code Red” Worm
<http://www.cert.org/advisories/CA-2001-23.html>
- CERT Advisory CA-2001-26 Nimda Worms
<http://www.cert.org/advisories/CA-2001-26.html>
- Step 3** If you are affected, continue to the next procedure.
-

Use the following procedure to clean the Nimda and Code Red Virus from the Cisco CallManager and Cisco CallManager Applications Servers.

Procedure

-
- Step 1** Perform an MCS Backup using Cisco-provided Cisco MCS Backup Utility. If you already have a known good backup, continue to the next step.
- Step 2** Ensure you do not have shared drives to any machines that are infected, because the worm can spread via shared drives.
- Step 3** Stop the IIS Admin service on the machine that is infected. (This will also stop the WWW publishing services.)
- Step 4** Download and run the **win-OS-Upgrade.3-1-1.EXE** that is available on CCO. This will require a reboot.



Note To see the link to the download, you must be a registered user to log in.

- Step 5** As a precaution for possible Code Red II vulnerabilities, download the Code Red II Cleanup tool from Microsoft at:
<http://download.microsoft.com/download/iis50/Tool/1.0/NT45/EN-US/CodeRedCleanup.exe>



Note Several antivirus companies have produced tools to eliminate Nimda; however, Cisco has tested the following tool and confirmed that it cleans a Cisco CallManager with no damaging side effects.

- Step 6** Download the Nimda Cleanup tool from Network Associates
<http://www.mcafee2b.com/naicommon/avert/avert-research-center/tools.asp#NimdaScn>
 Scroll to the bottom of the page and download **Nimdascn.zip** (440 Kb).
- Step 7** Navigate to the directory where the CodeRedCleanup.exe was placed and run it: **CodeRedCleanup.exe**.
- Step 8** Unzip the Nimda Cleanup Tool and place the files along with the Code Red II Cleanup tool on the hard drive of the affected machine.
- Step 9** Choose **Start > Run** and enter **cmd.exe**.
 Navigate to the directory where you placed the Nimda and Code Red II Cleanup tools.
- Step 10** Run the Nimda Cleanup Tool by entering **nimdascn c:*.***

- Step 11** After this action completes, do the same for the E drive: **nimdasnc e:*.***
Cisco CallManager should only have a C and E drive as hard drives with D being the CD-ROM drive.
- Step 12** If the server has any other hard drives, run **nimdasnc** for those drives, as well.
-

Find more details on viruses, their effect on Cisco equipment, as well as vulnerabilities on the PSIRT Advisories web page at the following URL:

<http://www.cisco.com/warp/public/707/advisory.html>

For more information on quick recovery from the Code Red II virus, see the Virus Protection section.

Verification

The Cisco CallManager service performs properly.

As a long-term solution, Cisco recommends the use of Cisco Host IDS Sensor and McAfee Netshield antivirus on the Cisco CallManager server. Both have been tested and approved for installation with the Cisco CallManager. Follow the recommended configuration settings to avoid undesired effects in the processor time.

You Are Not Authorized to View This Page

Symptom

When accessing the administration page, the following error message displays.

Error Message You Are Not Authorized to View This Page
and other similar error messages that may occur include

- You do not have permission to view this directory or page using the credentials you supplied.
- HTTP 401.3 Access denied by ACL on resource Internet Information Services.

- Server Application Error. The server has encountered an error while loading an application during the processing of your request. Please refer to the event log for more detailed information. Please contact the server administrator for assistance.
- Error: Access is Denied.

Probable Cause

The NTFS permissions have been modified on your C drive off the root directory to propagate into child directories on the Cisco CallManager server.

NTFS permissions have been changed from the default settings on the server and are no longer sufficient for IIS to run properly.

Corrective Action

Visit the Microsoft site for details on the issue: Q271071 “Minimum NTFS Permissions Required for IIS 5.0 to Work” at the following URL:

<http://support.microsoft.com/default.aspx?ln=EN-GB&pr=kbinfo&>

Verification

Use the following procedure to verify that IIS is started.

Procedure

-
- Step 1** From the Start menu, choose **Start > Programs > Administration Tools > Services**.
 - Step 2** Right-click the service.
 - Step 3** Verify the status, which should display Started.
 - Step 4** If any service is stopped, perform the following procedures to start the service(s).
-

Use the following procedure to start the IIS.

**Note**

If the IIS is stopped, the WWW publishing services may also be stopped. Start the WWW publishing services, which starts the IIS automatically.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

A window displays listing IIS Admin Service.

Step 2 Right-click **IIS Admin Service**.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The IIS starts.

Start the other services using the following procedure.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

Step 2 Right-click the service.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The service starts.

Errors Occur When Attempting to Access the Cisco CallManager Administration Page from a Browser on a Remote Server

If you can access the Administration Web page locally on the Cisco CallManager server, but not when you browse from a remote machine, verify whether one of the following situations applies to you. They appear in order, from the most frequent reason to the least frequent reason.

Name to Address Resolution Failing

Symptom

One of the following error messages displays when you try to access the following URL:

`http://your-cm-server-name/ccmadmin`

- Internet Explorer: This page cannot be displayed
- Netscape: Not Found. The requested URL /ccmadmin was not found on this server.

If you try to access the same URL using the Cisco CallManager IP address (`http://10.48.23.2/ccmadmin`) instead of the name, the page displays.

Probable Cause

The name that you entered as "your-cm-server-name" is mapping to the wrong IP address in DNS or hosts file.

Corrective Action

Procedure

-
- Step 1** If you have configured the use of DNS, check in the DNS to see whether the entry for the *your-cm-server-name* has the correct IP address of the Cisco CallManager server. If it is not correct, change it.

- Step 2** If you are not using DNS, your local machine will check in the "hosts" file to see whether there is an entry for the *your-cm-server-name* and an IP address associated to it. Open the file and add the Cisco CallManager server name and the IP address.

You can find the "hosts" file at `C:\WINNT\system32\drivers\etc\hosts` on your Windows station.

Default Web Site Under IIS Has Improper Setting

Symptom

One of the following error messages displays when you try to access the following URL:

`http://your-cm-server-name/ccmadmin`

- Internet Explorer: This page cannot be displayed
- Netscape: Not Found. The requested URL /ccmadmin was not found on this server.

If you try to access the same page using the Cisco CallManager IP address (`http://10.48.23.2/ccmadmin`) instead of the name, the page displays.

Probable Cause

An incorrect setting in the **Default Web Site** tab for the IIS has been set on the server.

Corrective Action

Procedure

- Step 1** Verify in the Internet Service Manager on the Cisco CallManager machine the **Default Web Site**. In the **Web Site** tab, choose **All Unassigned** and not the IP address of the machine.

You can verify that setting by choosing **Start > Programs > Administrative tools/Internet Service Manager**. Expand the icon that shows your server name.

- Step 2** Right-click **Default Web Site**. You have option properties that you must choose. Look for the **Web Site** tab and verify the **All Unassigned** setting.

**Note**

If you need to keep the specific IP address setting for any reason, you will not be able to use the name instead of IP address from a remote web browser.

Port 80 Is Blocked in One or More Routers Between Your Local Browser and the Cisco CallManager Server

Symptom

One of the following error messages displays when the port that is used by the web server or the http traffic is being blocked by a firewall:

- Internet Explorer: This page cannot be displayed
- Netscape: There was no response. The server could be down or is not responding

Probable Cause

For security reasons, the http access from your local network to the server network has been blocked.

Corrective Action

Procedure

- Step 1** Verify whether other types of traffic to the Cisco CallManager server are allowed, such as ping or Telnet. If any of them are successful, it will show that http access to the Cisco CallManager Web server has been blocked from your remote network.
- Step 2** Check the security policies with your network administrator.
- Step 3** Try again from the same network where the Server is located.
-

You Attempt to Access a Machine Where Access Is Explicitly Denied

Symptom

One of the following error messages displays:

- Internet Explorer: This page cannot be displayed
- Netscape: Not Found. The requested URL / ccmadmin was not found on this server.
- From both browsers without **show friendly http error messages** advance setting configured: Access to this server is forbidden.

Probable Cause

This represents a security policy that is applied by the network administrator.

Corrective Action

Procedure

- Step 1** Check the security policies with your network administrator. Try again from a different machine.
 - Step 2** If you are the network administrator, check the **Directory Security** tab of the **Default Web Site** in the Internet Service Manager on the Cisco CallManager server.
 - Step 3** You can verify the setting by choosing **Start > Programs > Administrative tools/Internet Service Manager**.
 - Step 4** Expand the icon that shows your server name.
 - Step 5** Right-click **Default Web Site**. You have the option properties from which you must choose.
 - Step 6** Look for the **Directory Security** tab and verify the setting.
-

Improper Network Setting Exists in the Remote Machine From Where You Are Browsing

Symptom

There is no connectivity, or there is no connectivity to other devices in the same network as the Cisco CallManager.

When you attempt the same action from other remote machines, the Cisco CallManager Administration Page displays.

Probable Cause

Improper network configuration settings on a station or on the default Gateway can cause a web page not to display because partial or no connectivity to that network exists.

Corrective Action

Procedure

- Step 1** Try pinging the IP address of the Cisco CallManager server and other devices to confirm that you cannot connect.
- Step 2** If the connectivity to any other device out of your local network is failing, check the network setting on your station, as well as the cable and connector integrity.
- Step 3** If the connectivity to any other device out of your local network is failing, check the network setting on your station, as well as the cable and connector integrity. Refer to the appropriate hardware documentation for detailed information.
- If you are using TCP-IP over a LAN to connect, continue with the following steps to verify the network settings on the remote station.
- Step 4** Choose **Start > Setting > Network and Dial-up connections**.
- Step 5** Choose **Local Area Connection**, then **Properties**.
- The list of communication protocols will appear checked.
- Step 6** Choose **Internet Protocol (TCP-IP)** and click **Properties** again.
- Step 7** Depending on your network, choose either **Obtain an ip address automatically** or **set manually your address, mask and default Gateway**.
- The possibility exists that a browser-specific setting could be improperly configured.
- Step 8** Choose the Internet Explorer browser **Tools > Internet Options**.
- Step 9** Choose the **Connections** tab and then verify the LAN settings or the dial-up settings.
- By default, the LAN settings and the dial-up settings are not configured. The generic network setting from Windows is used.
- Step 10** If the connectivity is failing only to the Cisco CallManager network, a routing issue probably exists in the network. Contact the network administrator to verify the routing that is configured in your default gateway.

**Note**

If you cannot browse from the remote server after following this procedure, contact TAC to have the issue investigated in more detail.

Refer to the following URL for more information on configuration settings:
http://www.cisco.com/warp/public/63/initial_config.shtml

Replication Fails Between the Publisher and the Subscriber

Symptom

Error Message Cannot update data because the publisher is not available. Please try again later. (58)

Probable Cause

The subscriber build failed.

Corrective Action

Procedure

- Step 1** Ensure that the NetBIOS name resolution is working between all servers.
- Step 2** Ensure (by editing) that the hosts and LMHOSTS are filled in on the publisher and subscriber servers, so each one can resolve the other's host name and NetBIOS name.
- Hosts is used for DNS resolution. LMHOSTS uses NetBIOS for name resolution. Also, SQL uses NetBIOS for name resolution.

If the Cisco CallManager fails to update, the database layer on the subscriber cannot find the publisher.

- Step 3** Check the SQL “distribution agent” on the publisher for history and errors.
- Step 4** Choose **Start > Programs > Administrative Tools > Local Security Policy**.
- Step 5** Choose **Audit Policy**.
- Step 6** Enable **Failure auditing for all events**.

For SQL, enable **Authentication**.



Note Users get replicated in the DC Directory, not in SQL.

- Step 7** From the web, upgrade the Cisco CallManager for the software version on your publisher.

The software will download the SQL database to the subscriber(s).

Slow Server Response

Symptom

Slow response from the server occurs.

Probable Cause

Slow response could result if the duplex of the switch does not match the duplex port setting on the Cisco CallManager server.

Corrective Action

Procedure

- Step 1** For optimal performance, set both switch and server to **100/Full**.
Cisco does not recommend using the Auto setting on either the switch or the server.
- Step 2** You must restart the Cisco CallManager server for this change to take effect.
-

Security

This section covers the following security issues and provides information on where to find detailed documentation regarding the security process:

- Changing IIS Parameters for Security
- Near-Term Security Solutions
- Long-Term Security Solutions
- Related Information

Changing IIS Parameters for Security

Symptom

You lose settings for locking down the IIS servers to protect the Cisco CallManager from hackers, attacks, or threats.

Probable Cause

Whenever you upgrade or reinstall the Cisco CallManager, all the IIS settings revert to the Cisco CallManager defaults.

Corrective Action

Test all your settings on a non-production Cisco CallManager before changing the settings on your production server.

Note the settings, because they will change every time that you perform an upgrade or reinstall, and you will have to reset them.

**Caution**

Ensure that you do not change any settings within the Cisco web directory, or you run the risk of losing a Cisco CallManager service due to a missing or moved file.

Near-Term Security Solutions

Refer to the following documents to ensure that you have quality of service (QoS) configured properly throughout your network to help ensure voice quality is affected as little as possible during the remainder of cleanup operations:

- *Cisco IP Telephony QoS Design Guide*
- *Cisco IP Telephony Network Design Guide*
- *IP Telephony Solutions Guide*

The following URL provides the guides:

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

Refer to the *Cisco IP Telephony Network Design Guide* to establish separate Voice/Data VLANs.

**Note**

This could provide a long-term solution depending on the size and complexity of the network involved.

Long-Term Security Solutions

After the immediate emergency is over, consult the *Cisco IP Telephony Solution Guide: Security Considerations for IP Telephony Networks* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/solution/4_design.htm

The subsection “Securing CallManager Servers” provides details on how to properly secure an IP Telephony solution for long term. The *Cisco IP Telephony Solution Guide* provides measures that would prevent Code Red issues on the Data network from affecting the IP telephony network.

Related Information

The following URL provides *Cisco CallManager Security Patch Process*:

http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/cmspp_qa.pdf

Cisco highly recommends that you do not install any patches from Microsoft. Download the wrapped versions from CCO.

You can sign up for Microsoft security patch alerts at the following URL:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp>

The alerts include an associated rating, which allows you an approximate time of a HotFix posting to CCO.

Refer to the following URL for security considerations for an IP telephony network:

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/solution/4_design.htm#22024

Virus Protection

This section covers the Code Red II Recovery procedures to immediately eliminate most of the effects to Cisco CallManager due to a widespread Code Red II infection.

See the A Virus is Affecting the Server Performance section for additional information.

Code Red II Recovery

Symptom

The worm can compromise the system and loads malicious commands or code.

Probable Cause

An email attachment carried the worm.

Corrective Action

Procedure

- Step 1** Run **win-OS-Upgrade.3-1-1.exe** (available from the Crypto Site) on all IP telephony servers that are running Windows 2000
- Step 2** Run the appropriate repair utility (Microsoft has a tool available) and/or manually (tool available from McAfee) close the back doors created by Code Red II.
- Step 3** For IP telephony servers that are running NT4.0 IIS, install Service Pack 6a and then the Code Red fix.



Caution

Due to the nature of this worm of creating backdoors, if this server is directly attached to the Internet, someone could have placed more back doors into it while it was compromised. If the possibility of the server being further compromised from within your network exists, the safest action would be to back up the data, and reinstall the server from scratch.

Stop Services

- Step 4** Stop and disable IIS Admin Service and World Wide Web Publishing service on all Cisco CallManager subscribers and any server that does not require the services.



Note

Ensure that these services remain active on the Cisco CallManager publisher server.

- Step 5** Bring up the services applet by choosing **Start > Programs > Administrative Tools > Services**.
- Step 6** Right-click **IIS Admin Service** and choose **Stop**.
This will also stop the World Wide Web Publishing service.
- Step 7** Right-click **IIS Admin Service** and choose **Properties**.
- Step 8** Change **Startup Type** to **Disable** and close the window.
- Step 9** Right-click **World Wide Web Publishing** and choose **Properties**.
- Step 10** Change **Startup Type** to **Disable** and close the window.
- Step 11** Patch/repair all known IIS servers in the network.

Deploy updated phone loads



Note 3.2(x) and 3.3(x) systems include all the necessary fixes and do not require an update phone load.

- Step 12** For 3.0(x) systems, download **cisocm_3-0-11_spA.exe** from CCO.
- Step 13** From Cisco CallManager Administration, go to **System > Device Defaults** and set the 7940/7960 Device Loads to **P003E310**.
- Step 14** Click **Update**.
- Step 15** For 3.1(x) systems, download **cisocm_3-1-1_spA.exe** from CCO.
- Step 16** From Cisco CallManager Administration, choose **System > Device Defaults** and set the 7940/7960 Device Loads to **P00303010100**.
- Step 17** Click **Update**.
- Step 18** Go to **System > CallManager Group**, choose the first group on the left side, and click **Reset Devices**.
- Step 19** When prompted, choose **OK**.

Repeat steps 12 through 19 for each Cisco CallManager Group that is present for the phones to get new loads.

Identify and Repair Remaining Infected IIS Servers

- Step 20** Identify and repair remaining infected IIS servers on the network (this could easily stretch into a near-term solution depending on how many "rogue" IIS servers are on the network).

Two methods follow to locate and repair infected IIS servers.

- Step 21** On the Cisco CallManager publishing server, or any other IIS server with logging enabled, go to C:\winnt\system32\logfiles\w3svc1 and get the most recent logfile. These files have a naming convention of ex000000.log.
- Step 22** Look for a line similar to the following one:

```
2001-08-09 00:11:57 172.20.148.189 - 172.20.225.130 80 GET
/default.ida
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXX
XX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u
7801%u9090%u9090%u8190%u
00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a200 -
```

In this case, the IP address 172.20.148.189 represents the attacking server.

- Step 23** Patch and clean or disconnect the server from the network.
- Step 24** Follow steps 21 through 23 until all remaining Code Red infected servers have been located and repaired.
- Step 25** Another method is to use the free utility available from eEye - CodeRedScanner. The utility will scan 1 Class C at a time looking for infected machines and machines that are vulnerable to an .ida based attack. A Class B scanner is available at additional cost.

■ Virus Protection



Directory Issues

This chapter covers the solutions for the most common issues related to a Cisco CallManager DC Directory (DCD), which uses a Lightweight Directory Access Protocol (LDAP) directory, and the Microsoft Active Directory (AD).

This chapter covers the following directory issues:

- DC Directory Stability
- Resolving Replication Problems Between DC Directory Servers in a Cisco CallManager Cluster
- Application Profiles Are Not Shown for User Configuration with the DC Directory
- Users List Is Not Visible from the Cisco CallManager Administration or Basic User Search Returns Nothing
- Add a New User Does Not Work and You Cannot Access the DC Directory Administrator

If the following procedures do not solve your directory issues, contact TAC for a more detailed investigation.



Caution

Using Katakana, Cyrillic, or other double-byte character sets with DC Directory, Netscape Directory, or Active Directory can cause directory database errors. This release of Cisco CallManager does not support using any double-byte character set with any directory.

For IP phone directory issues, refer to the following URL for detailed information:

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

DC Directory Stability

Symptom

The following issues relate to the instability of the DCD:

- You cannot to add a user or view the Global Directory.
- The DCD service stops.
- The DCD services on the publisher server and the subscriber server may not be synchronized.

Probable Cause

The DCD server stops and does not restart.

Corrective Action

Use the following procedure to stabilize the DCD.

**Note**

You must perform the following steps for each server.

**Note**

Cisco recommends that you schedule a downtime to run these procedures.

Procedure

- Step 1** Choose **Start > Settings > Control Panel**.
- Step 2** Choose **Administrative Tools**.
- Step 3** Click the **Services** icon.

- Step 4** Click **DC Directory Service**.
 - Step 5** In the General Tab, ensure the Service type is set to **Automatic**.
 - Step 6** In the Recovery tab, ensure that all three failure responses are set to **Restart the Service**.
 - Step 7** Click **OK** to close the DCD Server Properties window.
 - Step 8** If the DCD is stopped, right-click the **DCD Service** and click **Start**.
-

After you complete the previous procedure, use the following procedure on the Cisco CallManager publisher server.

Procedure

- Step 1** Choose **Start > Run**.
- Step 2** At the prompt, enter **cmd**.
- Step 3** Change the directory to **C:\dcdsrvr\bin**.
- Step 4** Enter **avvid_save** to save the data on the publisher server.
- Step 5** Stop the DCD Services by right-clicking **DC Directory Server** and click **Stop**.
- Step 6** At the prompt, enter **cleandsa** to clean the DCD server.
- Step 7** Right-click **DC Directory Server** and click **Start**.
- Step 8** At the prompt, enter **avvid_cfg publisher | current database in use** to reconfigure the DCD server on only the publisher server.

Replace *publisher* for your publisher name and *current database in use* for the name of your current database.



Note

To find your current database, choose **Start > Programs > SQL Server > Enterprise Manager**. Click the tree to your publisher. Click the database folder. The last listed number specifies the current database in use by your Cisco CallManager.

- Step 9** At the prompt, enter **avid_restore** to restore the DCD server data
- Step 10** Close the Command Prompt and Services Manager Windows.
-

After you complete the previous procedures, continue with the following procedure on all Cisco CallManager subscriber servers.



Note Ensure that you can ping between your Cisco CallManager publisher server and all Cisco CallManager subscriber servers because network connectivity is crucial for the following procedure.



Note Do not perform this procedure from a Terminal Services Window.



Note Using the following procedure, you must issue the commands on each subscriber server.

Procedure

- Step 1** Choose **Start > Run**.
- Step 2** At the prompt, enter **cmd**.
- Step 3** Change the directory to **C:\dcdsrvr\bin**.
- Step 4** Stop the DCD Services by right-clicking **DC Directory Server** and click **Stop**.
- Step 5** At the prompt, enter **cleandsa** to clean the DCD server.
- Step 6** Right-click **DC Directory Server** and click **Start**.
- Step 7** At the prompt, enter **avid_scfg publisher | subscriber** to reconfigure the DCD server on all subscriber servers where *publisher* is the name of your publisher server and *subscriber* is the name of your subscriber server.
- Step 8** At the prompt, enter **avid_restore** to restore the DCD server data.
- Step 9** Close the Command Prompt and Services Manager Windows.
-

Verification

Use the following procedure to verify that the DCD is stable and efficiently running.

Procedure

-
- Step 1** From Cisco CallManager Administration, choose **User > Global Directory**.
- Step 2** Search for users.
-

Resolving Replication Problems Between DC Directory Servers in a Cisco CallManager Cluster

The following procedures explain how to resolve directory replication problems between DC Directory Server services running on Cisco CallManager servers involved in a cluster.

- Backing Up Your Existing Data on the Publisher
- Reconfiguring DC Directory on the Publisher Server
- Re-initializing the LDAP Replication Partnership on the Subscriber Servers

Symptom

The publisher Cisco CallManager server has correct user data, and one or more subscriber Cisco CallManager servers either do not have user data or the user data is out of synchronization.

Probable Cause

Incorrect configuration probably causes the problem.

Corrective Action

Perform the following procedures from the console of the MCS (Media Convergence Server), connected through a Keyboard/Video/Mouse (KVM) switch, or connected via Telnet to the servers.

Do not perform these specific tasks while connected through a Terminal Services Client connection.

Backing Up Your Existing Data on the Publisher

Backing up your existing data on the publisher ensures that your user data in DC Directory on the publisher Cisco CallManager server is backed up in case of a failure during the following procedures.

Procedure

-
- Step 1** On the publisher server, while logged in as the Administrator, open a command prompt by choosing **Start > Run**.
 - Step 2** Enter **cmd**.
 - Step 3** Enter the command **avvid_save**.
 - Step 4** When prompted, press any key.



Note If IP Auto Attendant or IP IVR data is not installed, errors display after "Saving Apps20 Information." This is expected.

- Step 5** Continue to the Reconfiguring DC Directory on the Publisher Server procedure.
-

Reconfiguring DC Directory on the Publisher Server

Perform the following procedure from the command prompt on the publisher server while logged in as the Administrator.

Procedure

- Step 1** On the publisher server, while logged in as the Administrator, open a command prompt by choosing **Start > Run**.
- Step 2** Enter **cmd**.
- Step 3** Enter the command: **net stop dcdirectory** to stop the DC Directory on the subscriber Cisco CallManager servers.
- Step 4** Enter the command **cleandsa**.
- Step 5** When prompted, press any key.
- Step 6** Enter the command **avvid_cfg**.
- Step 7** Enter the command **avvid_restore**.
- Step 8** When prompted, press any key.
- The publisher's DC Directory is reconfigured and has all the data that it did at the time the **avvid_save** command was run.
- Step 9** Continue to the Re-initializing the LDAP Replication Partnership on the Subscriber Servers procedure.
-

Re-initializing the LDAP Replication Partnership on the Subscriber Servers

If you followed the previous steps, the DC Directory Server service should already be stopped on the subscriber servers. Use the following procedure to re-initialize the LDAP replication partnership on the subscriber servers.

Procedure

- Step 1** From a command prompt on the subscriber server, logged in as the Administrator, enter the command **cleandsa**.
- Step 2** When prompted, press any key.
- Step 3** Enter the command **avvid_scfg publisher | subscriber** where *publisher* is the Windows computer name of the publisher server and *subscriber* is the Windows computer name of the subscriber server where the command is being executed.



Note The publisher should be able to ping the subscriber by the name specified with this command, and the subscriber should be able to ping the publisher by the name specified in this command. If pings by these names are failing, Cisco recommends that you either point the servers to a valid WINS server if one exists in the network or manually configure LMHOSTS files on each.

Step 4 Repeat all steps on each subscriber server.

Verification

Use the following procedure to verify that each subscriber server has the same DC Directory data as the publisher server.

Procedure

- Step 1** From Cisco CallManager Administration, choose **User > Global Directory**.
- Step 2** To test replication agreements, make a change on one server and check another server to make sure that the change has been replicated.
-

Application Profiles Are Not Shown for User Configuration with the DC Directory

Symptom

When you are adding a user to the directory, the Application Profiles (such as AutoAttendant, Softphone, and Extension Mobility) do not display, and a user cannot be linked to those profiles.

Probable Cause

The Application Profiles were configured incorrectly.

Corrective Action

Use the following procedure to configure the application profile, so you can add or view users in the DC Directory.

Procedure

- Step 1** Connect to the **DC Directory Administrator**.
- Step 2** Choose **Directory > cisco.com > CCN**.
- Step 3** Click **systemProfile**.
- Step 4** Right-click **systemProfile** and choose **Properties**.
- Step 5** Click the **Application Install Status** tab.
- Step 6** Check the values for the applications. If the values for “AA Installed,” “Softphone Installed,” “ASR Installed,” and “Hotelling Installed” are blank, go to Step 7. Otherwise, proceed to Step 11.
- Step 7** Choose **Modify**.
- Step 8** Change the values from true to **false** and those that are false to **true**.
- Step 9** Click **Apply**.
- Step 10** Click **OK**.
- Step 11** Repeat Step 4 and Step 5.
- Step 12** Click **Modify**.
All values should be visible.
- Step 13** Change the value of the installed applications to **true**.
- Step 14** Click **Apply**.
- Step 15** Click **OK**.
- Step 16** Click **Services**.
- Step 17** In the right panel, choose **World Wide Web Publishing Service**.

- Step 18** Click the **Restart Service** icon.
- Step 19** Repeat all steps for all servers in the cluster in which you experienced the problem.
-

Verification

The Application Profiles display in the DC Directory.

Users List Is Not Visible from the Cisco CallManager Administration or Basic User Search Returns Nothing

Symptom

You cannot add a user or search for a user from Cisco CallManager Administration.

Adding a new user returns the following error.

Error Message Sorry your session object has timed out. Click here to Begin a New search.

Searching for a new user results in the page refreshing and waiting for input.

Probable Cause

Your Cisco CallManager host name contains an invalid DNS character.

Corrective Action

Do one of the following steps:

- Do not use non-DNS characters in the server name.

- If the server name contains non-DNS characters, use the IPAddress to browse the system.
- Use a Netscape or Internet Explorer browser that does not have the Q313675 patch.

Add a New User Does Not Work and You Cannot Access the DC Directory Administrator

Symptom

You cannot add a user from Cisco CallManager Administration. Also, cannot log in to the DC Directory Administrator.

Probable Cause

The Directory Manager user password contains special characters, such as “^”.

Corrective Action

Use the following procedure to change the DC Directory password to one that does not contain special characters.



Note

You must have superuser account privileges before you can change the DC Directory Manager password.



Note

When you have a publisher server and one or more subscriber servers in a cluster, you must perform the steps in the following procedures on all Cisco CallManagers within the cluster.

Procedure

- Step 1** From Cisco CallManager Administration, choose **Start > Programs > DC Directory Administrator**.

- Step 2** Click **Next**.
- Step 3** In the Password field, enter the default password, `cisco`, and click **Finish**.
The DC Directory Administrator window displays.
- Step 4** From the Tools menu, choose **Change Password**.
The Change User Password window appears.
- Step 5** In the Old Value field, enter `cisco`.
- Step 6** In the New Value field, enter a new `password`, without special characters.
- Step 7** In the Confirm New Value field, reenter your new `password`.
- Step 8** Click **OK**.
The DC Directory password is changed.
- Step 9** Continue with Configuring the Windows Registry.
-

Cisco CallManager Administration also uses the Directory Manager account to perform add, remove, or update operations on the DC Directory LDAP server.

Configuring the Windows Registry

Use the following procedure to update the information that is stored in the registry to ensure that the registry is pointing to the correct directory.

Procedure

- Step 1** Open a command line and enter `c:\dcdsrvr\bin`.
- Step 2** Enter the passwordutils.exe password.
`passwordutils.exe password`
- Step 3** Press **Enter**.
You need the Encrypted Password value information for the registry.
- Step 4** Choose **Start > Run**.
- Step 5** In the Open field, enter `regedit`.
The Registry Editor window displays.

- Step 6** Go to My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Directory Configuration.
LDAPURL must point to the correct directory.
`ldap://host:port`
- Step 7** Double-click **DCDMGRPW**.
The Edit String window appears.
- Step 8** In the Value Data field, enter the Encrypted Password value that you obtained in Step 3.
- Step 9** Click **OK**.
- Step 10** From the Registry Editor window, double-click **MGRPW**.
The Edit String window appears.
- Step 11** In the Value Data field, enter the Encrypted Password value that you obtained in Step 3.
- Step 12** Click **OK**.
You have successfully changed the password in the registry.

**Note**

After changing the registry entries, you must restart the WWW and IIS services on the Cisco CallManager node to pick up the latest settings from the registry.

- Step 13** Choose **Control Panel > Administrative Tools**.
- Step 14** Double-click **Services**.
The Services window displays.
- Step 15** Choose **Worldwide Web Publishing Service**.
- Step 16** Click **Stop**.
- Step 17** Click **Start**.
- Step 18** Choose **DC Directory Server**.
- Step 19** Click **Stop**.
- Step 20** Click **Start**.

If you use CRA 2.x that connects to the DC Directory, you must update the password in the Application Administration pages. Continue with Reconfiguring the Directory Manager Password for CRA and E-services.

Reconfiguring the Directory Manager Password for CRA and E-services

If you use CRA 2.x that connects to the DC Directory, use the following procedure to update the password in the Application Administration pages.

Procedure

- Step 1** Enter **http://servername/AppAdmin** where *servername* is the DNS name or IP address of your application server.
 - Step 2** When prompted, enter the *network user name* and *password*.
 - Step 3** Choose **Directory Configuration**.
The Directory Configuration window appears.
 - Step 4** In the Directory Password field, enter your new *password*.
 - Step 5** Click **OK**.
-

Verification

To verify that you successfully changed the Cisco CallManager DC Directory Manager password, use the following procedure.

Procedure

- Step 1** From Cisco CallManager Administration, choose **User > Global Directory**.
The User Information window appears.

Step 2 Click **Search**.

Step 3 If you can view the users that are configured in the system, the configuration was successful.

If you cannot view the users that are configured in the system, verify the following information:

- The new password is effective: Log in to the DC Directory with the new password.
- The encrypted password was entered correctly into the registry.
- The directory is pointing to the correct directory and not another directory (such as AD or an old directory which could be empty).
- The Worldwide Web Publishing and DC Directory services are restarted and running after the restart.

Related Information

For directory installation and configuration information, go to the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_3/install



Device Issues

This chapter addresses the following common problems that you may experience with Cisco IP Phones, gateways, and related devices.

- Voice Quality
- Codec and Region Mismatches
- Location and Bandwidth
- Phone Resets
- Dropped Calls
- Gateway Reorder Tone
- Gateway Registration Failure
- Gatekeeper Issues
- B-Channel Remains Locked When Restart_Ack Does Not Contain Channel IE

Voice Quality

You may experience voice quality issues including lost or distorted audio signal during phone calls.

Common problems include audio breaks (like broken words) or the presence of odd noises and audio distortion, such as echo, and watery or robotic voice quality. One-way audio, that is, a conversation between two people where only one person can hear anything, does not actually represent a voice quality issue, but this section covers this issue.

You may experience audio problems with one or more of the following items:

- Gateways
- Phones
- Networks

This section covers the following common voice quality problems:

- Lost or Distorted Audio
- Correcting Audio Problems from the Cisco IP Phone
- Echo
- One-Way Audio or No Audio

Lost or Distorted Audio

Symptom

One of the most common problems that you may encounter involves broken audio signal (often described as garbled speech or lost syllables within a word or sentence). Two common causes for this exist: packet loss and/or jitter. Packet loss means that audio packets do not arrive at their destination because they were dropped or arrived too late to be useful. Jitter describes the variation in the arrival times of packets. In the ideal situation, all Voice over IP (VoIP) packets would arrive exactly at a rate of 1 every 20 microseconds (ms). Notice that this is not the it takes for a packet to get from point A to point B but is simply the variation in packet arrival times.

Probable Cause

Many sources of variable delay exist in a network. You can control some of these but not others. You cannot entirely eliminate variable delay in a packetized voice network. Digital Signal Processors (DSP) on phones and other voice-capable devices by design buffer some of the audio in anticipation of variable delay. This dejittering occurs only when the audio packet has reached its destination and is now ready to be put into a conventional audio stream.

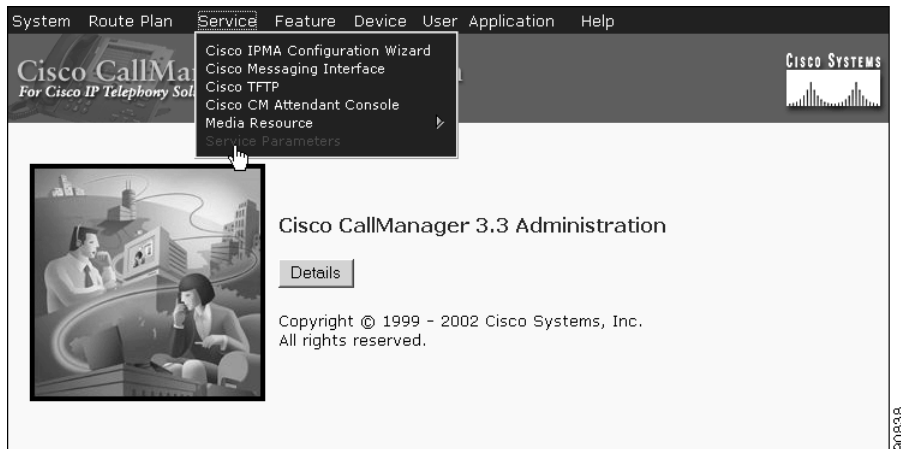
The Cisco IP Phone 7960 can buffer as much as 1 second of voice samples. The jitter buffer is adaptive, meaning if a burst of packets is received, the Cisco IP Phone 7960 can play them out in an attempt to control the jitter. The network administrator needs to minimize the variation between packet arrival times by applying quality-of-service (QoS) and other measures in advance (especially if calls cross a WAN).

Corrective Action

Procedure

- Step 1** When you are faced with a lost or distorted audio problem, first try to isolate the path of the audio. Try to identify each network device (switches and routers) in the path of the call audio stream. Keep in mind that the audio may be between two phones, or between a phone and a gateway, or it could have multiple legs (from a phone to a transcoding device and from there to another phone). Try to identify whether the problem occurs only between two sites, only through a certain gateway, on a certain subnet, and so on. This will help narrow the number of devices that you need to look at more carefully.
- Step 2** Next, disable silence suppression (also known as Voice Activation Detection or VAD). This mechanism does save bandwidth by not transmitting any audio when there is silence but may cause noticeable or unacceptable clipping at the beginning of words.
- Disable the service in Cisco CallManager Administration, choose **Service > Service Parameters**. From there, choose the server and the Cisco CallManager service as shown in Figure 6-1.

Figure 6-1 Cisco CallManager Administration Service Menu



- Step 3** Set SilenceSuppression to **False** to disable for all devices in a Cisco CallManager cluster; alternatively, you can set SilenceSuppressionForGateways to **False**. When in doubt, turn both off by choosing the value **False** for each.
- Step 4** Using a network analyzer, if a network analyzer is available, check whether a monitored call between two phones has 50 packets per second (or 1 packet every 20 ms) when silence suppression is disabled. With proper filtering, you can identify whether an excessive number of packets are lost or delayed.

Remember that delay by itself will not cause clipping, only variable delay. Notice in the table below, which represents a perfect trace, the arrival times between the audio packets (which will have an RTP header) that will be 20 ms. In a poor quality call (such as a call with a lot of jitter), the arrival times would vary greatly.

The following table illustrates a perfect trace.

Packet Number	Time - absolute (sec)	Time - delta (ms)
1	0	
2	0.02	20
3	0.04	20
4	0.06	20
5	0.08	20

Placing the packet analyzer into various points in the network will help narrow the number of places from which the delay is coming from. If no analyzer is available, you will need to use other methods. Examine interface statistics of each device in the path of the audio.

Diagnostic Call Detail Records (CDR) specifies another tool for tracking calls with poor voice quality. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information about CDRs.

Correcting Audio Problems from the Cisco IP Phone

Symptom

Audio problems occurs while a call is in progress.

Probable Cause

Devices, where a higher speed interface feeds into a lower speed interface, provide the most common sources for delay and packet loss. For example, a router may have a 100 Megabyte (MB) fast Ethernet interface connected to the LAN and a slow frame-relay interface, connected to the WAN. If the poor audio quality occurs only when communicating to the remote site, the most likely causes of the problem include

- The router has not been properly configured to give voice traffic priority over data traffic.
- Too many active calls exist for the WAN to support (that is, no call admission control restricts the number of calls that can be placed).
- Physical port errors occur.
- Congestion in the WAN itself occurs.

On the LAN, the most common problems represent physical-level errors (such as CRC errors) that are caused by faulty cables, interfaces, or by incorrectly configured devices (such as a port speed or duplex mismatch). Make sure that the traffic is not crossing any shared-media device, such as a hub.

Corrective Action

The Cisco IP Phone 7960 provides another tool for diagnosing possible audio problems.

Procedure

-
- Step 1** On an active call, you can press the *i* button twice rapidly and the phone will display an information screen that contains packet receive and transmit statistics, as well as average and maximum jitter counters.



Note On this screen, jitter represents the average of the last five packets that arrived; the maximum jitter designates the maximum for the average jitter.

- Step 2** Situations could also occur where the traffic is taking a slower path through the network than expected. If QoS has been configured correctly, the possibility exists that there is no call admission control. Depending on your topology, you can accomplish this through the use of **Locations** in Cisco CallManager Administration configuration, or by using a Cisco IOS router as a gatekeeper. In any case, you should always know the maximum calls supported across your WAN.

Diagnosing Crackling Sounds

- Step 3** Crackling is another poor quality symptom, which is sometimes caused by a defective power supply or some kind of strong electrical interference close to the phone. Try swapping the power supply and moving the phone.

Checking Your Loads

- Step 4** Verify gateway and phone loads. Check Cisco Connection Online (CCO) at www.cisco.com for the latest software loads, new patches, or release notes relating to the problem.
-

Verification

Procedure

- Step 1** Test by disabling silence suppression as described in Lost or Distorted Audio; then, place calls between the two sites. Do not place the calls on hold or on mute because this will stop packets from being transmitted.
- Step 2** With the maximum number of calls across the WAN, the calls should all have acceptable quality.
- Step 3** Test to make sure that a fast busy is returned when you try to make one more call.
-

Echo

Symptom

Echo occurs when the speech energy being generated and transmitted down the primary signal path is coupled into the receive path from the far end. The speaker then hears his or her own voice, delayed by the total echo path delay time.

Voice can reflect back. This can happen but goes unnoticed in a traditional voice network because the delay is so low. To the user, it sounds more like a side-tone than an echo. In a VoIP network, it will always be noticeable because packetization and compression contribute to the delay.

Probable Cause

Remember that the cause of the echo is always with analog components and wiring. For instance, IP packets cannot simply turn around and go back to the source at a lower audio level or on digital T1/E1 circuits. The only exception may occur if one party is using a speakerphone that has the volume set too high or other situations where an audio loop is created.

Corrective Action

Procedure

- Step 1** Make sure that the problem phones are not using the speakerphone and that they have the headset volume set to reasonable levels (start with 50 percent of the maximum audio level). Most of the time, the problems occur when you attach to the PSTN by way of a digital or analog gateway.

Testing the Gateway

- Step 2** Determine which gateway is being used. If a digital gateway is in use, you may be able to add additional padding in the transmit direction (towards the PSTN). Because lower signal strength will yield less reflected energy, this should clear the problem.

Additionally, you can adjust the receive level, so any reflected audio is reduced even further. Remember to make small adjustments at a time. Too much attenuation of the signal will make the audio impossible to hear on both sides.

- Step 3** Alternatively, you can contact the carrier and request to have the lines checked. On a typical T1/PRI circuit in North America, the input signal should be -15 dB. If the signal level is much higher (-5 dB, for example), echo likely will result.

Keeping an Echo Log

- Step 4** You should keep a log of all calls that experience echo.

Record the time of the problem, the source phone number, and the number called. Gateways have a fixed time of 16 ms of echo cancellation.

If the delay in the reflected audio is longer than this, the echo cancellor cannot work properly. This should not be an issue for local calls, and long distance calls should have external echo cancellers built into the network at the Central Office. This fact provides one of the reasons why it is important to note the external phone number of a call that experiences echo.

Checking Your Loads

- Step 5** Verify your gateway and phone loads. Check Cisco Connection Online at www.cisco.com for the latest software loads, new patches, or release notes that may relate to the problem.
-

One-Way Audio or No Audio

Symptom

When one person cannot hear another person during a call, one-way audio exists.

Probable Cause

An improperly configured Cisco IOS Gateway, a firewall, or a routing or default gateway problem, among other things can cause this problem.

Corrective Action

Procedure

- Step 1** You may find that diagnostic Call Detail Records (CDR) are useful for determining whether a call is experiencing one-way audio because they log transmitted and received packets (see *Lost or Distorted Audio* and refer to the *Cisco CallManager Serviceability Administration Guide* for more details.).
- You can also press the **i** button twice quickly on a Cisco IP Phone 7960 during an active call to view details about transmitted and received packets.

Checking the MTP

- Step 2** If you are using Media Termination Point (MTP) in a call (to support supplementary services such as hold and transfer with H.323 devices that do not support H.323 version 2), check to see whether the allocated MTP is working correctly. Cisco IOS routers support H.323 version 2 beginning in Cisco IOS Releases 11.3(9)NA and 12.0(3)T. Starting with Cisco IOS Release 12.0(7)T, the optional H.323 Open/Close LogicalChannel is supported, so software-based MTP is no longer required for supplementary services.

You can use the MTP device, as well as Conference Bridge and transcoder features, to bridge two or more audio streams. If the MTP, Conference Bridge, or transcoder is not working properly, you may experience one-way audio or audio loss. Shut down MTP to find out whether MTP is causing the problem.

Testing Cisco CallManager Configuration

- Step 3** Many causes exist for one-way audio or loss of audio during a call. An improperly configured device provides the most common cause. For instance, Cisco CallManager handles the call setup for a Cisco IP Phone. The actual audio stream occurs between the two Cisco IP Phones (or between the Cisco IP Phone and a gateway). The Cisco CallManager can signal to a destination phone (making it ring) when the phone originating the call does not have an IP route to the destination phone. A common cause for this happens when the default gateway in the phone is improperly configured either manually or on the DHCP server.

If a call consistently has one-way audio, use a PC that is configured on the same subnet as the phone and has the same default gateway and try to ping the destination Cisco IP Phone.

- Step 4** Using a PC that is configured on the same subnet as the destination phone (with the same default gateway as the destination phone) ping the source phone.

- Step 5** Other things that can affect the audio traffic include a firewall or a packet filter (such as access lists on a router) that may be blocking the audio in one or both directions. If the one-way audio occurs only through a voice-enabled Cisco IOS gateway, check the configuration carefully.

Ensure that IP routing is enabled (look at the configuration to make sure that no IP routing is not found near the beginning of the configuration).

Checking RTP Header Compression

- Step 6** Make sure that if you are using RTP header compression to save bandwidth across the WAN, that it is enabled on each router that is carrying voice traffic that attaches to the WAN circuit. A situation should not occur where the RTP header is compressed on one end but cannot be decompressed on the other side of the WAN. Sniffer is a very useful tool when troubleshooting one-way audio problems because you can verify whether the phone or gateway is actually sending or receiving packets.

**Note**

When a call is muted, no packets get transmitted from the phone that has pressed the **Mute** button. The **Hold** button stops the audio stream, so no packets get sent in either direction. When the **Hold** button is released, all the packet counters are reset. Remember that Silence Suppression must be disabled on both devices for the TX and RX counters to stay equal. Disabling Silence Suppression system-wide will not affect Cisco IOS gateways.

Codec and Region Mismatches

If a user gets a reorder tone (busy signal) when going off hook, it could be the result of codec disagreement between regions. Verify that both call ends support at least one common codec (for example, G.711). If they do not, you will need to use transcoders.

A region specifies the range of supported codecs that can be used with each of the other regions. Every device belongs to a region.

**Note**

Codec negotiation with a Cisco IOS router is not supported.

For example, Region1<->Region2 = G.711, means that a call between a device in Region1 and a device in Region2 can use G.711 or any other supported codec that requires the same or less bandwidth as G.711 (any supported codecs within G.711, G.729, G.723, and so on).

**Note**

The following list gives codecs that are supported for each device:
Cisco IP Phone 7960—G.711A-law/μ-law, G.729AnnexB
Cisco IP Phone SP12 series and VIP 30—G.711a-law/mu-law, G.723.1
Cisco Access Gateway DE30 and DT-24+—G.711a-law/mu-law, G.723.1

Location and Bandwidth

If a user gets a reorder tone after dialing a number, this could happen because the Cisco CallManager bandwidth allocation for the location of one of the call end devices has been exceeded. Cisco CallManager checks for 24k available bandwidth for each device before making a call. If less than 24k bandwidth is available, Cisco CallManager will not set up the call, and the user receives a reorder tone.

```
12:42:09.017 Cisco CallManager|Locations:Orig=1 BW=12Dest=0 BW=-1 (-1
implies infinite bw available)
12:42:09.017 Cisco CallManager|StationD - stationOutputCallState
tcpHandle=0x4f1ad98
12:42:09.017 Cisco CallManager|StationD - stationOutputCallInfo
CallingPartyName=, CallingParty=5003, CalledPartyName=,
CalledParty=5005, tcpHandle=0x4f1ad98
12:42:09.017 Cisco CallManager|StationD - stationOutputStartTone:
37=ReorderTone tcpHandle=0x4f1ad98
```

Once the call is established, the Cisco CallManager will subtract bandwidth from the locations, depending on the codec used in that call. If the call is using G.711, Cisco CallManager will subtract 80k; if the call is using G.723, Cisco CallManager will subtract 24k; if the call is using G.729, Cisco CallManager will subtract 24k.

Phone Resets

Symptom

Phone resets.

Probable Cause

Phones will power cycle or reset for two reasons:

- TCP failure connecting to Cisco CallManager
- Failure to receive an acknowledgement to the phone KeepAlive messages.

Corrective Action

Procedure

- Step 1** Check the phones and gateways to ensure that you are using the latest software loads.
- Step 2** Check Cisco Connection Online at www.cisco.com for the latest software loads, new patches, or release notes that may relate to the problem.
- Step 3** Check the Event Viewer for instances of phone(s) resetting. Phone resets represent considered Information events.
- Step 4** Look for any errors that may have occurred around the time that the phone(s) reset.
- Step 5** Start an SDI trace and try to isolate the problem by identifying any common characteristics in the phones that are resetting. For example, check whether they are all located on the same subnet, same VLAN, and so on. Look at the trace and determine:
- If the resets occur during a call or happen intermittently
 - If there any similarities of phone model (such as Cisco IP Phone 7960 or Cisco IP Phone 30VIP)
- Step 6** Start a Sniffer trace on a phone that frequently resets. After it has reset, look at the trace to determine if there are any TCP retries occurring. If so, this indicates a network problem. The trace may show some consistencies in the resets, such as the phone resetting every seven days. This might indicate DHCP lease expiration every seven days (this value is user-configurable; for example, it could be every two minutes).
-

Dropped Calls

Symptom

Premature termination of dropped calls.

Probable Cause

Premature termination of dropped calls can be the result of a phone or gateway resetting (see Phone Resets) or a circuit problem, such as incorrect PRI configuration.

Corrective Action

Procedure

- Step 1** Determine whether this problem is isolated to one phone or to a group of phones. Perhaps you will find that the affected phones are all on a particular subnet or location.
- Step 2** Check the Event Viewer for phone or gateway resets.
- You will see one Warning and one Error message for each phone that resets. This indicates that the phone cannot keep its TCP connection to the Cisco CallManager alive, so the Cisco CallManager resets the connection. This may occur because a phone was turned off or a problem may exist in the network. If this is an intermittent problem, you may find it useful to use Microsoft Performance to record phone registrations.
- Step 3** If the problem seems to be occurring only through a certain gateway, such as a Cisco Access DT-24+, the best course of action is to enable tracing and/or view the Call Detail Records (CDR). The CDR files will give a cause of termination (CoT) that may help determine the cause of the problem. Refer to the *Cisco CallManager Serviceability Administration Guide* for detailed information on CDRs.
- Step 4** Find the disconnect cause values (origCause_value and destCause_value—depending on which side hung up the call), that map to Q.931 disconnect cause codes (in decimal) at the following location:
- <http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/dbook/disdn.htm>.

- Step 5** If the call is going out of a gateway to the PSTN, you can use the CDR to determine which side is hanging up the call. Obtain much of the same information by enabling tracing on the Cisco CallManager. Because the trace tool can affect Cisco CallManager performance, you will want to use this option only as a last resort or if your network is not yet in production.
-

Gateway Reorder Tone

Symptom

Reorder tone occurs.

Probable Cause

Users placing a call through the gateway might get a reorder tone if they are attempting to make a restricted call or to call a number that has been blocked. A reorder tone may occur if the dialed number is out of service or if the PSTN has an equipment or service problem.

Check to be sure that the device giving the reorder tone has registered. Also, check your dial plan configuration to ensure that the call can be successfully routed.

Corrective Action

The following procedure shows the steps for troubleshooting reorder tones through gateways.

Procedure

- Step 1** Check the gateways to ensure that you are using the latest software loads.
- Step 2** Check Cisco Connection Online at www.cisco.com for the latest software loads, new patches, or release notes relating to the problem.

- Step 3** Start an SDI trace and re-create the problem. Reorder tones could be the result of a configuration issue with location-based admission control or gatekeeper-based admission control where the Cisco CallManager might limit the number of allowable calls. In the SDI trace, locate the call to determine if it was blocked intentionally by a route pattern or the calling search space or by any other configuration setting.
- Step 4** Reorder tones can also occur when calling occurs through the PSTN. Check the SDI trace for Q.931 messages, in particular for disconnect messages. If a Q.931 disconnect message is present, it means that the other party caused the disconnect, and you cannot correct for that.
-

Gateway Registration Failure

This section describes two similar but different categories of gateways. The Cisco Access AS-X, AT-X and Cisco Access DT-24+ and DE-30+ belong to one category. These gateways identify stand-alone units that are not directly connected to a Network Management Processor (NMP). The second category includes the Analog Access WS-X6624 and Digital Access WS-X6608. These gateways, as blades installed in a Catalyst 6000 chassis, provide direct connectivity to the NMP for control and stuning.

Symptom

A registration problem represents one of the most common issues that are encountered with gateways on a Cisco CallManager.

Probable Cause

Registration can fail for a variety of reasons.

Corrective Action

Procedure

- Step 1** First, check that the gateway is up and running. All gateways have a heartbeat LED that blinks 1-second-on, 1-second-off when the gateway software is running normally.
- If this LED is not blinking at all, or blinking very rapidly, the gateway software is not running. Normally, this results in an automatic reset of the gateway. Also, it is normal for the gateway to reset itself if it cannot complete the registration process after about 2 to 3 minutes. So, you may happen to look at the heartbeat LED while the device is resetting, but if the normal blinking pattern does not appear in 10 to 15 seconds, the gateway has suffered a serious failure.
- On the Cisco Access Analog gateways, find the green heartbeat LED on the far right of the front panel. On the Cisco Access Digital gateways, find the red LED on the far left on the top edge of the card. On the Cisco Analog Access WS-X6624, a green LED appears inside the blade (not visible from the front panel) on the far right card edge near the front. Finally, on the Digital Access WS-X6608, a separate heartbeat LED exists for each of the 8 spans on the blade. Eight red LEDs appear across the card (not visible from the front panel) about two thirds of the way towards the back.
- Step 2** Check that the gateway received its IP address. A standalone gateway must receive its IP address via DHCP or BOOTP. A Catalyst gateway may receive its IP address by DHCP, BOOTP or by manual configuration through the NMP.
- Step 3** If you have access to the DHCP server, the best way to check a standalone gateway is to verify that the device has an outstanding lease on an IP address. If the gateway shows up on your server, this provides a good indication but is not definitive. Delete the lease at the DHCP server.
- Step 4** Reset the gateway.
- Step 5** If the gateway reappears on the server with a lease within a couple of minutes, everything works fine in this area. If not, either the gateway cannot contact the DHCP server (Is a router improperly configured and not forwarding DHCP broadcasts? Is the server running?) or cannot get a positive response (Is the IP address pool depleted?).
- Step 6** If performing these checks does not yield the answer, use a sniffer trace to determine the specific problem.

- Step 7** For a Catalyst 6000 gateway, you should check to make sure that the NMP can communicate with the gateway. You can check this by trying to ping its internal IP address from the NMP.

The IP address uses this format:

```
127.1.module.port
```

For example, for port 1 on module 7, you would enter

```
Console (enable) ping 127.1.7.1
127.1.7.1 is alive
```

- Step 8** If pinging works, the **show port** command shows the IP address information. Make sure that the IP address information and the TFTP IP address is correct as well.
- Step 9** If the gateway is failing to obtain valid DHCP information, use the **tracy** utility (supplied by Cisco TAC) to determine the problem.
- Step 10** After obtaining this utility from TAC, issue the following command from the Cat6000 Command Line Interface (CLI):

```
tracy_start mod port
```

In this example, the WS-X6624 represents module 7, and it has only a single 860 processor, so it is port 1. The command to issue is **tracy_start 7 1**.

The following output actually comes from the 860-console port on the gateway board itself; however, the output of the **tracy** command represents nothing more than a remote copy of the 860-console port.

```

      |           |
      | |       | | | | | |
      | | |     | | |
      | | | |   | | | |
      | | | | | | : : | | | | | | | | : :
C i s c o   S y s t e m s
CAT6K Analog Gateway (ELVIS)
APP Version : A0020300, DSP Version : A0030300, Built Jun  1 2000
16:33:01

```

```

ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE
00:00:00.050 NMPTask:got message from XA Task
00:00:00.050 (NMP) Open TCP Connection ip:7f010101
00:00:00.050 NMPTask:Send Module Slot Info
00:00:00.060 NMPTask:get DIAGCMD
00:00:00.160 (DSP) Test Begin -> Mask<0x00FFFFFF>

```

```
00:00:01.260 (DSP) Test Complete -> Results<0x00FFFFFF/0x00FFFFFF>
00:00:01.260 NMPTask:get VLANCONFIG
00:00:02.870 (CFG) Starting DHCP
00:00:02.870 (CFG) Booting DHCP for dynamic configuration.
00:00:06.570 (CFG) DHCP Request or Discovery Sent, DHCPState =
INIT_REBOOT
00:00:06.570 (CFG) DHCP Server Response Processed, DHCPState =
INIT_REBOOT
00:00:06.780 (CFG) IP Configuration Change! Restarting now...
00:00:10.480 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT
00:00:14.480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
00:00:22.480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
00:00:38.480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
```

If this timeout message continues to scroll by, a problem exists with contacting the DHCP server.

- Step 11** First, check that the Catalyst 6000 gateway port is in the correct VLAN. You will find this information in the information that you retrieved by using the **show port** command.
- Step 12** If the DHCP server is not on the same VLAN as the Catalyst 6000 gateway, then make sure that the appropriate IP helper addresses have been configured to forward the DHCP requests to the DHCP server. The gateway can get stuck in the INIT state after a VLAN number change until the gateway resets.
- Step 13** When in the INIT state, try resetting the gateway. Every time that the 860 gets reset, your tracy session will be lost, so you must close your existing session and reestablish a new one by issuing the following commands:

```
tracy_close mod port
```

```
tracy_start mod port
```

- Step 14** If you are still seeing the `DHCPState = INIT` messages, check whether the DHCP server is functioning correctly.
- Step 15** If so, start a sniffer trace to see whether the requests are being sent and the server is responding.

Once DHCP is working correctly, the gateway will have an IP address that allows the use of the tracy debugging utility. This utility includes a built in feature of the NMP command set for the Catalyst gateways and is available as a helper application that runs on Windows 98/NT/2000 for the standalone gateways.

Step 16 To use the helper application `tracy` utility, connect to the gateway by using the IP address to which it is assigned. This `tracy` application works on all the gateways, provides a separate trace window for each gateway (up to eight may be traced at once), and allows traces to be logged directly to a file that you specify.

Step 17 Verify that the TFTP server IP address was correctly provided to the gateway. DHCP normally provides DHCP in Option 66 (by name or IP address), Option 150 (IP address only), or `si_addr` (IP address only). If your server has multiple Options configured, `si_addr` will take precedence over Option 150, which will take precedence over Option 66.

If Option 66 provides the `DNS_NAME` of the TFTP server, then the DNS server(s) IP address(es) must have been specified by DHCP, and the name entered in Option 66 must resolve to the correct TFTP server IP address. The NMP could configure a Catalyst gateway could be configured by the NMP to disable DHCP, and the NMP operator must then manually enter all configuration parameters at the console, including the TFTP server address.

Additionally, the gateways will always attempt to resolve the name `CiscoCM1` via DNS. If successful, the `CiscoCM1` IP address will take precedence over anything that the DHCP server or NMP tells it for the TFTP server address, even if the NMP has DHCP disabled.

Step 18 You can check the current TFTP server IP address in a gateway by using the `tracy` utility. Enter the following command to get the configuration task number:

```
TaskID: 0  
Cmd:    show t1
```

Look for a line with `config` or `CFG` and use the corresponding number as the `taskID` for the next line, such as, for the Cisco Access Digital gateway. In the examples that follow, bolded lines of text make it easier for you to see the messages being explained. In the actual display output, text does not appear bolded. The examples come from an `WS-X6624` model; the command to dump the DHCP information is

```
TaskID: 6  
Cmd:    show dhcp
```

Step 19 The TFTP server IP address then appears. If it is not correct, verify that your DHCP options and other information that it provides are correct.

- Step 20** Once the TFTP address is correct, ensure that the gateway is getting its configuration file from the TFTP server. If you see the following information in the Tracy output, your TFTP service may not be working correctly, or the gateway might not be configured on the Cisco CallManager:

```
00:09:05.620 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP
Server
00:09:18.620 (CFG) TFTP Error: Timeout Awaiting Server Response for
.cnf File!
```

The gateway attempts to connect to the same IP address as the TFTP server if it does not get a configuration file. This works fine unless you are in a clustered environment in which the gateway needs to receive its list of redundant Cisco CallManagers.

- Step 21** If the card is not getting its TFTP information correctly, check the TFTP service on the Cisco CallManager and make sure it is running.

- Step 22** Check the TFTP trace on the Cisco CallManager.

Another common problem occurs if the gateway is not configured correctly on the Cisco CallManager. A typical error involves entering an incorrect MAC address for the gateway. If this is the case, for a Catalyst 6000 gateway, you will probably get the following messages on the NMP console every 2 minutes:

```
2000 Apr 14 19:24:08 %SYS-4-MODHPRESET:Host process (860) 7/1 got
reset asynchronously
2000 Apr 14 19:26:05 %SYS-4-MODHPRESET:Host process (860) 7/1 got
reset asynchronously
2000 Apr 14 19:28:02 %SYS-4-MODHPRESET:Host process (860) 7/1 got
reset asynchronously
```

The following example shows what the Tracy output would look like if the gateway is not in the Cisco CallManager database:

```
00:00:01.670 (CFG) Booting DHCP for dynamic configuration.
00:00:05.370 (CFG) DHCP Request or Discovery Sent, DHCPState =
INIT_REBOOT
00:00:05.370 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.370 (CFG) Requesting DNS Resolution of CiscoCM1
00:00:05.370 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.370 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.370 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP
Server
00:00:05.370 (CFG) TFTP Error: .cnf File Not Found!
00:00:05.370 (CFG) Requesting SAADefault.cnf File From TFTP Server
00:00:05.380 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.380 (CFG) Updating Configuration ROM...
```

```

00:00:05.610 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.610 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket
00:00:05.610 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:05.610 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:00:05.610 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.610 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =
SentRegister
00:00:05.680 GMSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPSocket
00:00:05.680 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
00:00:20.600 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:00:20.600 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket
00:00:20.600 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:20.600 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM

```

Another possible registration problem could be that the load information is incorrect or the load file is corrupt. The problem could also occur if the TFTP server is not working. In this case, tracy shows that the TFTP server reported that the file is not found:

```

00:00:07.390 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =
SentRegister
00:00:08.010 GMSG: TFTP Request for application load A0021300
00:00:08.010 GMSG: CCM#0 CPEvent = LOADID --> CPState = AppLoadRequest
00:00:08.010 GMSG: ***TFTP Error: File Not Found***
00:00:08.010 GMSG: CCM#0 CPEvent = LOAD_UPDATE --> CPState =
LoadResponse

```

In this case, the gateway requests application load A0021300, although the correct load name would be A0020300. For a Catalyst 6000 gateway, the same problem can occur when a new application load needs to get its corresponding DSP load as well. If the new DSP load is not found, a similar message will appear.

```

ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE
00:00:00.050 NMPTask:got message from XA Task
00:00:00.050 (NMP) Open TCP Connection ip:7f010101
00:00:00.050 NMPTask:Send Module Slot Info
00:00:00.060 NMPTask:get DIAGCMD
00:00:00.160 (DSP) Test Begin -> Mask<0x00FFFFFF>
00:00:01.260 (DSP) Test Complete -> Results<0x00FFFFFF/0x00FFFFFF>
00:00:01.260 NMPTask:get VLANCONFIG
00:00:02.030 (CFG) Starting DHCP
00:00:02.030 (CFG) Booting DHCP for dynamic configuration.
00:00:05.730 (CFG) DHCP Request or Discovery Sent, DHCPState =
INIT_REBOOT
00:00:05.730 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.730 (CFG) Requesting DNS Resolution of CiscoCM1

```

```

00:00:05.730 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.730 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.730 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP
Server
00:00:05.730 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.730 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.730 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket
00:00:05.730 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:05.730 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:00:05.730 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.730 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =
SentRegister
00:00:06.320 GMSG: CCM#0 CPEvent = LOADID --> CPState = LoadResponse
00:01:36.300 GMSG: CCM#0 CPEvent = TIMEOUT --> CPState = BadCCM
00:01:36.300 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
00:01:46.870 GMSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPSocket
00:01:51.300 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:01:51.300 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket
00:01:51.300 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:01:51.300 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:01:51.300 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:01:51.300 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =
SentRegister
00:01:51.890 GMSG: CCM#0 CPEvent = LOADID --> CPState = LoadResponse

```

The difference here is that the gateway gets stuck in the LoadResponse stage and eventually times out. You can resolve this problem by correcting the load file name in the Device Defaults area of Cisco CallManager Administration.

Gatekeeper Issues

Before starting any gatekeeper troubleshooting, verify that IP connectivity exists within the network. Assuming that there is IP connectivity, use the following information in this section to troubleshoot your gatekeeper calls:

- Intercluster Trunks or H.225 Trunks
- Admission Rejects
- Registration Rejects

Intercluster Trunks or H.225 Trunks

Refer to the *Cisco CallManager Administration Guide* and *Cisco CallManager System Guide* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_3/index.htm

Admission Rejects

Symptom

The system issues Admission Rejects (ARJ) when Cisco CallManager has registered with the Gatekeeper but cannot send a phone call.

Probable Cause

Configuration issues on the gatekeeper should be the primary focus when the gatekeeper issues an ARJ.

Corrective Action

Procedure

- Step 1** Verify IP connectivity from the Cisco CallManager to the gatekeeper.
 - Step 2** Show gatekeeper status and verify that the gatekeeper state is up.
 - Step 3** Is there a zone subnet defined on the gatekeeper? If so, verify that the subnet of the Cisco CallManager is in the allowed subnets.
 - Step 4** Verify that the technology prefix matches between the Cisco CallManager and the gatekeeper configuration.
-

Registration Rejects

Symptom

The system issues Registration Rejects (RRJ) when Cisco CallManager cannot register with the gatekeeper.

Probable Cause

Configuration issues on the gatekeeper should be the primary focus when the gatekeeper is issuing a RRJ.

Corrective Action

Procedure

- Step 1** Verify IP connectivity from the Cisco CallManager to the gatekeeper.
 - Step 2** Show gatekeeper status and verify that the gatekeeper state is up.
 - Step 3** Is there a zone subnet defined on the gatekeeper? If so, verify that the subnet of the gateway is in the allowed subnets.
-

Cisco CallManager Locks the B-Channel and Sends Restart

Symptom

Cisco CallManager locks the B-channel and sends a restart on that channel for no apparent reason. For related information, see B-Channel Remains Locked When Restart_Ack Does Not Contain Channel IE.

Outbound calls cause DSPs to lockup.

**Note**

Release 3.1(2c) Engineer Special 21 resolves this problem.

Probable Cause

Your ISDN channel selection order causes a glare condition. This may occur when a high volume of calls occurs.

Also, B-channel selection for outgoing calls is exclusive (the Cisco CallManager does not accept other B-channels). If a channel is not available, the PABX or CO sends Release Complete.

Corrective Action**Procedure**

- Step 1** From Cisco CallManager Administration, choose **Device > Gateway** as shown in Figure 6-2.

Figure 6-2 Cisco CallManager Administration Device Menu



The Find and List Gateways window displays.

- Step 2** Enter search criteria to locate a specific gateway as shown in Figure 6-3.

Figure 6-3 Find and List Gateways Window

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

Find and List Gateways [Add a New Gateway](#)

No current search

Find gateways where begins with

and show items per page. endpoints.

To list all items, click Find without any search text, or use "Device Name is not empty" as the search criteria.

No active query. Please enter your search criteria using the options above.

- Step 3** Click **Find**.
- A list of discovered devices displays.
- Step 4** Click the *device name* of the gateway that you want to update.
- The Gateway Configuration window appears.
- Step 5** To access gateway ports, click the icon of the gateway port or the MGCP endpoint link on the left side of the configuration window for the chosen gateway.
- Step 6** Check the **Inhibit Restarts at PRI initialization** check box as shown in Figure 6-4.

Figure 6-4 Interface Information Window

Interface Information	
PRI Protocol Type*	PRI NI2
Protocol Side*	User
Channel Selection Order*	Bottom Up
Channel IE Type*	Use Number when 1B
PCM Type*	μ-law
Delay for first restart (1/8 sec ticks)	32
Delay between restarts (1/8 sec ticks)	4
<input checked="" type="checkbox"/> Inhibit restarts at PRI initialization	
<input type="checkbox"/> Enable status poll	

- Step 7** Click **Update**.
- Step 8** Reset the gateway to apply the changes.
- Step 9** Restart the Cisco CallManager server.



Note You must restart the Cisco CallManager server to clear the restart problem after checking the **Inhibit Restarts at PRI Initialization** check box.

For detailed information on E1/T1 PRI configuration settings, refer to the *Cisco CallManager Administration Guide*.

B-Channel Remains Locked When Restart_Ack Does Not Contain Channel IE

Symptom

This issue relates to the previous issue: Cisco CallManager Locks the B-Channel and Sends Restart.

When the Cisco CallManager system receives a Release Complete with cause ie=channel not available, the system sends out a Restart to bring this channel back to the idle state.

Probable Cause

In the Restart, you specify with the Channel IE which channel(s) must be restarted. If the network responds with Restart_Ack without the Channel IE, the system keeps this channel in a locked state. While on network side, this same channel goes back to idle state.

Now you end up with the network requesting this channel for inbound calls.

Because the channel is locked on the Cisco CallManager server, the Cisco CallManager releases any call requests for this channel.

This behavior occurs on numerous sites in the UK and when the gateway is an E1 blade (most likely the same happens when using MGCP backhaul on the 2600/3600).

A glare condition provides the likely reason for the Release Complete.

You see this frequent happening on sites where a high call volume occurs.

If the B-channel selection on the network is top-down or bottom up, all inbound calls will fail until a B-channel in the higher/lower range is freed (if an active call gets cleared).

When B-channel selection is round-robin over a certain time, you will end up with an E1 blade with all locked B-channels.

Corrective Action

Reset the E1 port.

Verification

The B-channel(s) return to the idle state.



Dial Plans and Routing Issues

This chapter addresses the following common problems that you may experience with dial plans, route partitions, and calling search spaces.

- Route Partitions and Calling Search Spaces
- Dial Plans

Route Partitions and Calling Search Spaces

Route partitions inherit the error-handling capabilities for the Cisco CallManager software. That is, a console and SDI file trace are provided for logging information and error messages. These messages will be part of the digit analysis component of the traces. You must be sure that you know how the Partitions and Calling Search Spaces are configured and what devices are in each partition and its associated calling search space to determine the source of the problem. The Calling Search Space determines what numbers are available for making a call. The Partition determines allowable calls to a device or route list.

Refer to the route plan chapters in the *Cisco CallManager Administration Guide* and the *Cisco CallManager System Guide* for more information.

The following trace shows an example of a dialed number that is in the device Calling Search Space. For more detailed explanations about SDI traces, review the case studies in this document.

```
08:38:54.968 Cisco CallManager|StationInit - InboundStim -  
OffHookMessageID tcpHandle=0x6b88028  
08:38:54.968 Cisco CallManager|StationD - stationOutputDisplayText  
tcpHandle=0x6b88028, Display= 5000
```

```

08:38:54.968 Cisco CallManager|StationD - stationOutputSetLamp stim:
9=Line instance=1 lampMode=LampOn tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputCallState
tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD -
stationOutputDisplayPromptStatus tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD -
stationOutputActivateCallPlane tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")

```

In the Digit Analysis component of the previous trace, the pss (Partition Search Space, also known as Calling Search Space) gets listed for the device placing the call.

In the following trace, RTP_NC_Hardwood;RTP_NC_Woodland;Local_RTP represent the partitions that this device is allowed to call.

```

08:38:54.968 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:54.968 Cisco CallManager|StationD - stationOutputStartTone:
33=InsideDialTone tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 5 tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationD - stationOutputStopTone
tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5")
08:38:55.671 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:56.015 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 0 tcpHandle=0x6b88028
08:38:56.015 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="50")
08:38:56.015 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:56.187 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 0 tcpHandle=0x6b88028
08:38:56.187 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="500")
08:38:56.187 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:56.515 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 3 tcpHandle=0x6b88028

```

```
08:38:56.515 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5003")
08:38:56.515 Cisco CallManager|Digit analysis: analysis results
08:38:56.515 Cisco CallManager||PretransformCallingPartyNumber=5000
```

The key thing to note is that PotentialMatchesExist is the result of Digit Analysis of the numbers that were dialed until the exact match is found and the call is routed accordingly.

The following trace describes what happens when the Cisco CallManager is attempting to dial the directory number 1001 and it is not in the Calling Search Space for that device. Again, the key thing to note is that the digit analysis routine had potential matches until only the first digit was dialed. The route pattern associated with the digit 1 is in a partition that is not in the device calling search space, RTP_NC_Hardwood;RTP_NC_Woodland;Local_RTP. Therefore, the phone received a reorder tone (busy signal).

```
08:38:58.734 Cisco CallManager|StationInit - InboundStim -
OffHookMessageID tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputDisplayText
tcpHandle=0x6b88028, Display= 5000
08:38:58.734 Cisco CallManager|StationD - stationOutputSetLamp stim:
9=Line instance=1 lampMode=LampOn tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputCallState
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD -
stationOutputDisplayPromptStatus tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD -
stationOutputActivateCallPlane tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")
08:38:58.734 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:58.734 Cisco CallManager|StationD - stationOutputStartTone:
33=InsideDialTone tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 1 tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationD - stationOutputStopTone
tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="1")
08:38:59.703 Cisco CallManager|Digit analysis:
potentialMatches=NoPotentialMatchesExist
```

```
08:38:59.703 Cisco CallManager|StationD - stationOutputStartTone:  
37=ReorderTone tcpHandle=0x6b88028
```

Route partitions work by associating a partition name with every directory number in the system. The directory number can be called only if the calling device contains the partition within a list of partitions to which it is permitted to place calls—its partition search space. This provides for extremely powerful control over routing.

When a call is being placed, Digit Analysis attempts to resolve the dialed address only in those partitions that the partition search space specifies. Each partition name comprises a discrete subset of the global dialable address space. From each listed partition, Digit Analysis retrieves the pattern that best matches the sequence of dialed digits. Then, from among the matching patterns, Digit Analysis chooses the best match. If two patterns equally match the sequence of dialed digits, Digit Analysis breaks the tie by choosing the pattern associated with the partition listed first in the partition search space.

Dial Plans

Symptom

Problems occur when a number is dialed.

Probable Cause

A Dial Plan is a list of numbers and groups of numbers that tells the Cisco CallManager what devices (such as phones and gateways) to send calls to when a certain string of digits is collected. It is analogous to a static routing table in a router. Please be certain your dial plan concepts, basic call routing, and planning have been carefully considered and properly configured before trying to troubleshoot a potential dial plan issue. Very often, the problem lies with planning and configuration. Refer to the route plan configuration chapters in the *Cisco CallManager Administration Guide* for more information.

Corrective Action

Procedure

Step 1 Identify the Directory Number (DN) that is originating the call.

Step 2 Identify the Calling Search Space for this DN.

**Tip**

The Calling Search Space determines what numbers are available for making a call.

Step 3 If applicable, identify which device the Calling Search Space is associated with this DN. Make sure that you identify the correct device; because multiple line appearances are supported, it is possible to have the same DN on multiple devices. Note the device's Calling Search Space.

If this is a Cisco IP Phone originating the call, remember that a particular line (DN) and the device that line is associated with have Calling Search Spaces. They will be combined when making a call. For example, if line instance 1000 has a Calling Search Space of AccessLevelX and the Cisco IP Phone that has extension 1000 configured on it has AccessLevelY as its Calling Search Space, then when making a call from that line appearance, Cisco CallManager will search through partitions contained in Calling Search Space AccessLevelX and AccessLevelY.

Step 4 Identify which Partitions are associated with the Calling Search Space(s).

**Tip**

The Partition determines allowable calls to a device or route list.

Step 5 Identify to which Partition of the device the call should (or should not) go.

Step 6 Identify which number is being dialed. Note if and when the user is getting a secondary dial tone. Also note what they hear after all the digits have been entered (reorder, fast-busy). Does the user get the progress tones before expecting to hear anything? Make sure that callers wait at least 10 seconds after entering the last digit because they may have to wait for the interdigit timer to expire.

Step 7 Generate a Route Plan Report in Cisco CallManager Administration, and use it to examine all the route patterns for the partitions that are in the Calling Search Space for the problem call.

Step 8 If necessary, add or modify the Route Patterns or Route Filters.

- Step 9** If you can find the Route Pattern to which the call is being sent, note the Route List or Gateway to which the pattern points.
- Step 10** If it is a Route List, check which Route Groups are part of the list and which Gateway(s) is part of the Route Groups.
- Step 11** Verify that the applicable devices are registered with Cisco CallManager.
- Step 12** If a gateway has no access to Cisco CallManager exists, use the show tech command to capture and verify this information.
- Step 13** Pay attention to the @ sign. This macro can expand to include many different things. It is often used in combination with filtering options.
- Step 14** If a device is not part of a partition, it is said to be part of the Null or default partition. Every user should be able to call that device. The system always searches the Null partition last.
- Step 15** If you dial an outside number that is matching a 9.@ pattern and it takes 10 seconds before the call goes through, check the filtering options. By default, with a 9.@ pattern, when a 7-digit number is dialed, the Cisco IP Phone will wait 10 seconds before placing the call. You need to apply a Route Filter to the pattern that displays LOCAL-AREA-CODE DOES-NOT- EXIST and END-OF-DIALING DOES-NOT-EXIST.
-

Secure Dial Plan

Use partitions and calling search spaces, in addition to more common filtering based on sections of the @ macro (which stands for the North American Numbering Plan) in a route pattern, to configure Cisco CallManager to create a secure dialing plan for users. Partitions and Calling Search Spaces provide an integral part of security and are especially useful for multitenant environments and for creating an individual user level. Filtering, a subset of the Calling Search Space/Partition concept, can add additional granularity to the security plan.

Be advised that usually the last thing you want to do when trying to fix a filtering problem is to run an SDI trace. There is simply not enough information, and the potential for causing more harm is too great.



Cisco CallManager Services Issues

This chapter covers the solutions for the following most common issues related to Cisco CallManager services:

- Conference Bridge Issues
- Transcoding Issues
- MTP Resource Issues

Conference Bridge Issues

Symptom

Error Message No Conference Bridge Available

Probable Cause

This could indicate either a software or a hardware problem.

Corrective Action

Procedure

- Step 1** Check to see whether you have any available software or hardware Conference Bridge resources registered with Cisco CallManager.
- Step 2** Use either Microsoft Performance or the Admin Serviceability Tool to check the number of Unicast AvailableConferences.



Note Cisco CallManager Release 3.1 uses different names for counters and objects. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

The Cisco IP Voice Media Streaming application performs the conference bridge function. One software installation of Cisco IP Voice Media Streaming will support 16 Unicast Available Conferences (3 people/conference), as shown in the following trace.



Note The number of supported devices may vary with different Cisco CallManager releases. Refer to the Release 3.1 documentation at the following location:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm

```
10:59:29.951 Cisco CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB_kirribilli - Registered
- ConfBridges= 16, Streams= 48, tcpHandle=4f12738
10:59:29.951 Cisco CallManager|UnicastBridgeManager -
UnicastBridgeRegistrationReq - Device Registration Complete for Name=
Xoø ô%ø - DeviceType= 50, ResourcesAvailable= 16, deviceTblIndex= 0
```

One E1 port (WS-X6608-E1 card contains 8x E1 ports) provides five Unicast Available Conferences (max conference size = 6), as shown in the following trace.

```
11:14:05.390 Cisco CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB00107B000FB0 - Registered
- ConfBridges= 5, Streams= 16, tcpHandle=4f19d64
11:14:05.480 Cisco CallManager|UnicastBridgeManager -
UnicastBridgeRegistrationReq - Device Registration Complete for Name=
Xoø ô%ø - DeviceType= 51, ResourcesAvailable= 5, deviceTblIndex= 0
```

The following hardware trace on the Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Module indicates that the E1 port 4/1 in the card has registered as a Conference Bridge with Cisco CallManager.

```
greece-sup (enable) sh port 4/1
Port Name Status Vlan Duplex Speed Type
-----
4/1 enabled 1 full -Conf Bridge

Port DHCP MAC-Address IP-Address Subnet-Mask
-----
4/1 disable 00-10-7b-00-0f-b0 10.200.72.31 255.255.255.0

Port Call-Manager(s) DHCP-Server TFTP-Server Gateway
-----
4/1 10.200.72.25 - 10.200.72.25 -

Port DNS-Server(s) Domain
-----
4/1 - 0.0.0.0

Port CallManagerState DSP-Type
-----
4/1 registered C549

Port NoiseRegen NonLinearProcessing
-----
4/1 disabled disabled
```

- Step 3** Check the maximum number of users that are configured in your ad hoc or meet-me conference to determine whether the problem occurred because this number was exceeded.

Transcoding Issues

Symptom

You have installed a hardware transcoder in the Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Module, and it does not work as expected (you cannot make calls between two users with no common codec).

Probable Cause

You may not have any available transcoder resources registered with Cisco CallManager (must be hardware).

Corrective Action

Use Microsoft Performance or the Admin Serviceability Tool to check the number of MediaTermPointsAvailable that are available.



Note

Cisco CallManager Release 3.1 uses different names for counters and objects. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

One E1 port (WS-X6608-E1 card contains 8x E1 ports) provides transcoder/MTP resources for 16 calls, as shown in the following trace.



Note

The number of supported devices may vary with different Cisco CallManager releases. Refer to the Release 3.1 documentation at the following location: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm

```
11:51:09.939 Cisco CallManager|MediaTerminationPointControl -
Capabilities Received - Device= MTP00107B000FB1 - Registered -
Supports 16 calls
```

The following hardware trace on the Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Module indicates that the E1 port 4/2 in the card has registered as an MTP/transcoder with Cisco CallManager.

```
greece-sup (enable) sh port 4/2
Port  Name                Status      Vlan      Duplex Speed Type
-----
 4/2                enabled      1         full    - MTP

Port    DHCP    MAC-Address      IP-Address      Subnet-Mask
-----
 4/2    disable 00-10-7b-00-0f-b1 10.200.72.32    255.255.255.0

Port    Call-Manager(s)  DHCP-Server      TFTP-Server      Gateway
-----
 4/2    10.200.72.25    -                 10.200.72.25    -
```

```

Port      DNS-Server(s)      Domain
-----
4/2      -                  0.0.0.0

Port      CallManagerState  DSP-Type
-----
4/2      registered        C549

Port      NoiseRegen        NonLinearProcessing
-----
4/2      disabled          disabled

```

**Note**

You cannot configure the same E1 port for both Conference Bridge and Transcoder/MTP

To make a call between two devices that are using a low bit rate code (such as G.729 and G.723) that do not support the same codec, you need a transcoder resource.

Assume Cisco CallManager has been configured such that the codec between Region1 and Region2 is G.729. The following scenarios apply:

- If caller on Phone A initiates a call, Cisco CallManager realizes it is a Cisco IP Phone 7960, which supports G.729. After the digits have been collected, the Cisco CallManager determines that the call is destined for User D who is in Region2. Because the destination device also supports G.729, the call gets set up, and the audio flows directly between Phone A and Phone D.
- If a caller on Phone B, who has a Cisco IP Phone 12SP+, initiates a call to Phone D, this time the Cisco CallManager would realize that the originating phone only supports G.723 or G.711. Cisco CallManager would need to allocate a transcoding resource so audio would flow as G.711 between Phone B and the transcoder but as G.729 between the transcoder and Phone D. If no transcoder were available, Phone D would ring, but as soon as the call was answered, the call would disconnect.
- If a user on Phone B calls Phone F, which is a Cisco IP Phone 12SP+, the two phones would actually use G.723, even though G.729 is configured as the codec to use between the regions. G.723 gets used because both endpoints support it, and it uses less bandwidth than G.729.

MTP Resource Issues

Symptom

A call gets established, but supplementary services are not available.

Probable Cause

An MTP resource problem could provide the source of the transcoding problem if a call is established, but supplementary services are not available on an H.323 device that does not support H323v2.

Corrective Action

Procedure

- Step 1** Determine whether you have any available software or hardware MTP resources registered with Cisco CallManager.
- Step 2** Use Microsoft Performance or the Admin Serviceability Tool to check the number of MediaTermPointsAvailable.



Note Cisco CallManager Release 3.1 uses different names for counters and objects. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

Using MTP to support supplementary services with H.323 devices that do not support H.323v2 allows one MTP software application to support 24 calls as shown in the following trace.



Note The number of supported devices may vary with different Cisco CallManager releases. Refer to the Release 3.1 documentation at the following location:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm

```
10:12:19.161 Cisco CallManager|MediaTerminationPointControl -
Capabilities Received - Device= MTP_kirribilli. - Registered -
Supports 24 calls
```

One E1 port (WS-X6608-E1 card contains 8x E1 ports) provides MTP resources for 16 calls, as shown in the following trace.

```
11:51:09.939 Cisco CallManager|MediaTerminationPointControl -
Capabilities Received - Device= MTP00107B000FB1 - Registered -
Supports 16 calls
```

The following hardware trace from the Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Module indicates that the E1 port 4/2 in the card has registered as an MTP/transcoder with Cisco CallManager.

```
greece-sup (enable) sh port 4/2
Port Name Status Vlan Duplex Speed Type
-----
4/2 enabled 1 full - MTP

Port DHCP MAC-Address IP-Address Subnet-Mask
-----
4/2 disable 00-10-7b-00-0f-b1 10.200.72.32 255.255.255.0

Port Call-Manager(s) DHCP-Server TFTP-Server Gateway
-----
4/2 10.200.72.25 - 10.200.72.25 -

Port DNS-Server(s) Domain
-----
4/2 - 0.0.0.0

Port CallManagerState DSP-Type
-----
4/2 registered C549

Port NoiseRegen NonLinearProcessing
-----
4/2 disabled disabled
```

Step 3 In the Gateway Configuration screen of Cisco CallManager Administration, check to see whether the **Media Termination Point Required** check box is checked.

Step 4 Verify that Cisco CallManager has allocated the required number of MTP devices.

From the SDI file:

```
15:22:23.848 Cisco CallManager|MediaManager(40) started
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest -
Transcoder Enabled
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest -
party1(16777357), party2(16777358), proxies=1, connections=2, current
proxies=0
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest -
proxy connections
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest -
allocating MTP(ci=16777359)
15:22:23.848 Cisco CallManager|MediaManager -
wait_AllocateMtpResourceRes
15:22:23.848 Cisco CallManager|MediaManager -
wait_AllocateMtpResourceRes - start 2 connections
15:22:23.848 Cisco CallManager|MediaManager -
wait_AllocateMtpResourceRes - creating connection between
party1(16777357) and party2(16777359)
15:22:23.848 Cisco CallManager|MediaManager -
wait_AllocateMtpResourceRes - creating connection between
party1(16777358) and party2(16777359)
15:22:23.848 Cisco CallManager|MediaCoordinator -
wait_MediaCoordinatorAddResource - CI=16777359 count=1
15:22:23.848 Cisco CallManager|MediaCoordinator -
wait_MediaCoordinatorAddResource - CI=16777359 count=2
```



Voice Messaging Issues

This chapter covers the solutions for the following most common voice messaging issues:

- Voice Messaging
- Unity Issues

Voice Messaging

For extensive troubleshooting information for Cisco Unity voice messaging, refer to the *Cisco Unity Troubleshooting Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity31/tsg/index.htm

For all documentation related to Cisco Unity, refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm>

Voice Messaging Stops After 30 Seconds

Symptom

When running Cisco Unity 3.x with Cisco CallManager, a caller only has 30 seconds in which to leave a voice-mail message.

Probable Cause

This problem occurs when a caller is leaving a voice message and the call is terminated 30 seconds into the message. Reproduce this easily by dialing a valid extension/number and attempting to leave a voice message that is longer than 30 seconds.

Corrective Action

Procedure

- Step 1** To resolve this problem, verify that the Media Gateway Control Protocol (MGCP) is being used on the voice gateway.
- Step 2** If the MGCP is being used, add the **no mgcp timer receive-rtcp** command.
- Step 3** If MGCP is not on the voice gateway, enable Skinny traces for the Cisco Unity server and Cisco CallManager traces.

Refer to Configuring Unity Traces with MaestroTools.exe at the following URL: http://www.cisco.com/warp/public/788/AVVID/unity_trace_maestrotools.html for further information on configuring Skinny traces in Cisco Unity 3.x and later.

Beginning with Cisco Unity 3.1, the Cisco Unity Diagnostic Tool replaces MaestroTools. For further information on utilizing this tool, refer to Cisco Unity Diagnostic Tool at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity31/tsg/tsg31/tsg_0900.htm#xtocid13

Unity Issues

This section covers the following topics:

- Unity Does Not Roll Over: Receive Busy Tone
- Calls Forwarded to Voice Messaging Are Treated as a Direct Call to Unity
- Administrator Account Not Associated with Cisco Unity Subscriber
- Noise in Recorded Message on Cisco Unity 3.1.2 or 3.1.3

Unity Does Not Roll Over: Receive Busy Tone

Symptom

Unity does not get past the first line and will not roll over to the second port.

Example

```
Call 5000 from 1001
Get Unity
Place the call on Hold
Press New Call
Dial 5000
Get Busy tone
Press End Call
Press Resume Call
Press End Call
```

Probable Cause

Messaging Interface is configured with the same number as Unity (5000), and it is registering the intercept, so the call is hitting CMI.

Corrective Action

Check the CMI service parameters to ensure that the voicemaildn is not configured.

Calls Forwarded to Voice Messaging Are Treated as a Direct Call to Unity

Symptom

Unity version is 2.4.5.135, TSP is 6.0(1), and Cisco CallManager is 3.1(31)spD.

Calls from one IP phone to another that are forwarded to voice messaging get treated as a direct call to Unity from the phone that is making the call. However, this only occurs if the digits are dialed but works properly (receiving the called phone's greeting) if the Redial softkey is pressed.

Probable Cause

The logic in the TSP states that if the call is a forwarded call and the originalCalledPartyName is "Voicemail," then mark the call as a direct call. This was done for failover Unity systems using Cisco CallManager.

Corrective Action

Procedure

- Step 1** On the Cisco CallManager server, change the name of the Display field on the Cisco Voice Mail ports to anything other than "VoiceMail."
- Step 2** On the Unity server, add a new Registry string value of HKLM\Software\ActiveVoice\AvSkinny\voiceMail display Name= *anything other than VoiceMail*.
-

Administrator Account Not Associated with Cisco Unity Subscriber

Symptom

While attempting to access the System Administrator (SA) page, you receive an error stating that the administrator account is not associated with the Unity subscriber.

Probable Cause

Access was not configured for the user.

Corrective Action

Procedure

- Step 1** To gain appropriate rights to access the SA page, you must run the GrantUnityAccess utility. Locate this tool at **C:\commserver\grantunityaccess.exe**



Note For more information about the GrantUnityAccess utility, refer to *Granting Administrative Rights to Other Cisco Unity Servers* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity31/sag/sag312/sag_0255.htm#xtocid8

- Step 2** If you run this utility with no options, the instructions should display. The normal use of this tool provides the domain/alias of the account that is to have access to the SA, and then provides information about from which account to *copy* those rights.

For example, if the alias of the user to whom you want to give administration rights is TempAdministrator and your domain name is MyDOMAIN, you would use the following command at the DOS prompt:

GrantUnityAccess -u MyDOMAIN\TempAdministrator -s Installer -f.

The installer account designates a special account that always has administration rights but is not created in the directory itself; it is local to the SQL database only.

Noise in Recorded Message on Cisco Unity 3.1.2 or 3.1.3

Symptom

This problem occurs only if the registry setting values for Automatic Gain Control (AGC) are set incorrectly. The bad values are usually

- AGCsamplesize is 4e20 hex (20000 decimal) and should be 1f40 hex (8000 decimal).
- AGCgainthreshold is 28 hex (40 decimal) and should be 5 hex (5 decimal).

Probable Cause

In some cases on Cisco Unity 3.1.2 servers, and possibly 3.1.3 upgraded servers, the AGC registry settings are set to the incorrect values. These incorrect settings can cause loud white noise in the following situations:

- At the beginning of a message.
- Within the message when the user stops talking while recording the message.
- At the end of the message.

Corrective Action

Changing the registry settings to the correct values eliminates the problem. For detailed information, refer to the Cisco Unity product documentation at the following URL:

http://www.cisco.com/univered/cc/td/doc/product/voice/c_unity/index.htm



Opening a Case With TAC

When you open a case with the Cisco TAC, you must provide preliminary information to better identify and qualify the issue. You may need to provide additional information, depending on the nature of the issue. Waiting to collect the following information upon the engineer's request after opening a case inevitably results in resolution delay.

- Required Preliminary Information
 - Network Layout
 - Problem Description
 - General Information
- TAC Web
- CCO Cases
- Attachments
- Cisco Live!
- Remote Access

Required Preliminary Information

For all issues, always provide the following information to TAC. Collect and save this information for use upon opening a TAC case and update it regularly with any changes.

- Network Layout

- Problem Description
- General Information

Network Layout

A detailed description of the physical and logical setup, as well as all the following network elements involved in the voice network (if applicable):

- Cisco CallManager(s)
 - Version (from Cisco CallManager Administration choose **Details**)
 - Number of Cisco CallManagers
 - Setup (stand-alone, cluster)
- Unity
 - Version (from the Cisco CallManager Administration)
 - Integration type
- Applications
 - List of installed applications
 - Version numbers of each application
- IP/voice gateways
 - OS version
 - Show tech (IOS gateway)
 - Cisco CallManager load (Skinny gateway)
- Switch
 - OS version
 - VLAN configuration
- Dial plan—Numbering scheme, call routing

Ideally, submit a Visio or other detailed diagram, such as JPG. Using the whiteboard, you may also provide the diagram through a Cisco Live! session.

Problem Description

Provide step-by-step detail of actions that the user performed when the issue occurs. Ensure the detailed information includes

- Expected behavior
- Detailed observed behavior

General Information

Make sure that the following information is readily available:

- Is this a new installation?
- If this is a previous version of a Cisco CallManager installation, has this issue occurred since the beginning? (If not, what changes were recently made to the system?)
- Is the issue reproducible?
 - If reproducible, is it under normal or special circumstances?
 - If not reproducible, is there anything special about when it does occur?
 - What is the frequency of occurrence?
- What are the affected devices?
 - If specific devices are affected (not random), what do they have in common?
 - Include DNs or IP addresses (if gateways) for all devices that are involved in the problem.
- What devices are on the Call-Path (if applicable)?

TAC Web

Use TAC Web, a detailed collection of tools and technical documents written by TAC engineers, to analyze common issues and provide solutions. See the presentation covering TAC Web tools and content that is available to help you use this tool at the following URL:

<http://www.cisco.com/public/support/tac/home.shtml>

Before you contact TAC, view the voice messaging *Top Issues* at the following URL:

http://www.cisco.com/public/support/tac/top_issues.shtml

and Cisco CallManager technical tips at the following URL:

http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Software:Cisco_Call_Manager

CCO Cases

Opening a case through CCO gives it priority over all other case-opening methods. High priority cases (P1 and P2) provide an exception to this rule.

Use the Case Open Tool at the following URL and log in as a registered user:

http://www.cisco.com/public/news_training/whats_hot.shtml

Provide an accurate problem description when opening a CCO case. That description of the problem returns URL links that may provide you with an immediate solution.

If you do not find a solution to your problem, continue the process of sending your case to a TAC engineer.

Attachments

Attach reports to a case by sending an email to the engineer and attaching a zip file for documents larger than 100 Kb.

At the following URL, use the *Manage a TAC Case* section, *please login* link to log in as a registered user:

<http://www.cisco.com/public/support/tac/contact.shtml>

Cisco Live!

Cisco Live!, a secure, encrypted Java applet, allows you and your Cisco TAC engineer to work together more effectively by using Collaborative Web Browsing / URL sharing, whiteboard, Telnet, and clipboard tools.

Access Cisco Live! at the following URL:

<http://c3.cisco.com/>

Remote Access

Remote access provides you with the ability to establish Terminal Services (remote port 3389), HTTP (remote port 80), and Telnet (remote port 23) sessions to all the necessary equipment.



Caution

When setting up dial-in, do not use **login:cisco** or **password:cisco** because they constitute a vulnerability to the system.

You may resolve many issues very quickly by allowing the TAC engineer remote access to the devices through one of the following methods:

- Equipment with public IP address.
- Dial-in access—In decreasing order of preference: analog modem, Integrated Services Digital Network (ISDN) modem, virtual private network (VPN).
- Network Address Translation (NAT)—IOS and private Internet exchange (PIX) to allow access to equipment with private IP addresses.

Ensure that firewalls do not obstruct IOS traffic and PIX traffic during engineer intervention and that all necessary services, such as Terminal Services, start on the servers.

**Note**

TAC handles all access information with the utmost discretion, and no changes will be made to the system without customer consent.

Cisco Secure Telnet Structure

Cisco Secure Telnet offers Cisco Service Engineers (CSE) transparent firewall access to Cisco CallManager servers on your site.

Cisco Secure Telnet works by enabling a Telnet client inside the Cisco Systems firewall to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and maintenance of your Cisco CallManager servers without requiring firewall modifications.

**Note**

Cisco accesses your network only with your permission. You must provide a network administrator at your site to help initiate the process.

Firewall Protection

Virtually all internal networks use firewall applications to restrict outside access to internal host systems. These applications protect your network by restricting IP connections between the network and the public internet.

Firewalls work by automatically blocking TCP/IP connections that are initiated from the outside, unless the software is reconfigured to allow such access.

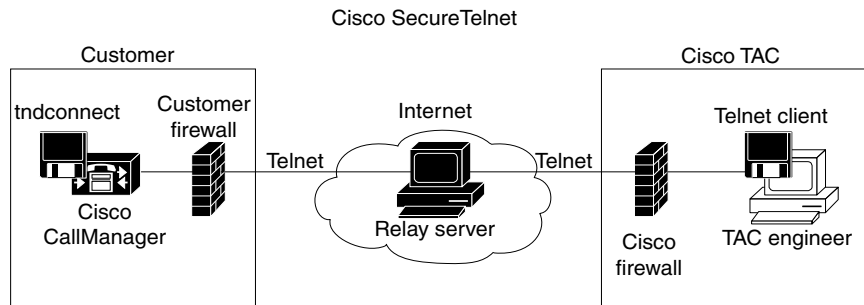
Corporate networks normally permit communication with the public Internet but only if connections directed to outside hosts originate from inside the firewall.

Cisco Secure Telnet Design

Cisco Secure Telnet takes advantage of the fact that Telnet connections can easily be initiated from behind a firewall. Using an external proxy machine, the system relays TCP/IP communications from behind your firewall to a host behind another firewall at the Cisco Technical Assistance Center (TAC).

Using this relay server maintains the integrity of both firewalls while supporting secure communication between the shielded remote systems.

Figure A-1 Cisco Secure Telnet System



34433

Cisco Secure Telnet Structure

The external relay server establishes the connection between your network and Cisco Systems by building a Telnet tunnel. This enables you to transmit the IP address and password identifier of your Cisco CallManager server to your CSE.



Note

The password comprises a text string upon which your administrator and the CSE mutually agree.

Your administrator starts the process by initiating the Telnet tunnel, which establishes a TCP connection from inside your firewall out to the relay server on the public Internet. The Telnet tunnel then establishes another connection to your local Telnet server, creating a two-way link between the entities.



Note

The Telnet client at the Cisco TAC runs in compliance with systems running on Windows NT and Windows 2000 or with UNIX operating systems.

After the Cisco CallManager at your site accepts the password, the Telnet client that is running at the Cisco TAC connects to the Telnet daemon that is running behind your firewall. The resulting transparent connection allows the same access as if the machine were being used locally.

Once the Telnet connection is stable, the CSE can implement all remote serviceability functionality to perform maintenance, diagnostic, and troubleshooting tasks on your Cisco CallManager server.

You can view the commands sent by the CSE and the responses issued by your Cisco CallManager server, but the commands and responses may not always be completely formatted.

Where to Find More Information

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide*.



Case Study: Troubleshooting Intracluster Phone Calls

The case study in this appendix discusses in detail the call flow between two Cisco IP Phones within a cluster, called an intracluster call. This case study also focuses on Cisco CallManager and Cisco IP Phone initialization, registration, and keepalive processes. A detailed explanation of an intracluster call flow follows the discussion. The explanation of the processes are explained using the trace utilities and tools discussed in Chapter 2, “Troubleshooting Tools”.

This appendix contains the following topics:

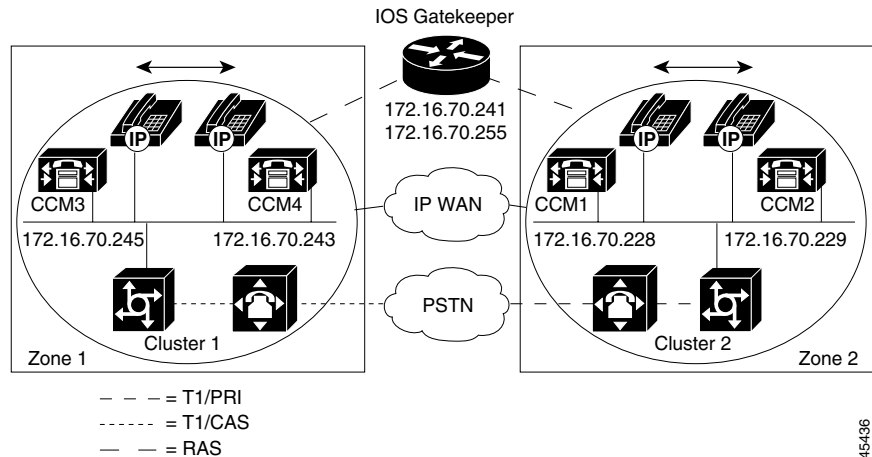
- Sample Topology
- Cisco IP Phone Initialization Process
- Skinny Station Registration Process
- Cisco IP Phone-to-Cisco IP Phone Call Flow Within a Cluster
- Cisco IP Phone-to-Cisco IP Phone Exchange of Skinny Station Messages During Call Flow
- Cisco CallManager Initialization Process
- Self-Starting Processes
- Cisco CallManager Registration Process
- Cisco CallManager KeepAlive Process
- Cisco CallManager Intracluster Call Flow Traces

Sample Topology

Given that you have two clusters named Cluster 1 and Cluster 2, the two Cisco CallManagers in Cluster 1 are called CCM3 and CCM4, while the two Cisco CallManagers in Cluster 2 are called CCM1 and CCM2.

The traces collected for this case study come from CCM1, which is located in Cluster 2, as shown in Figure B-1. The basis for the call flow are the two Cisco IP Phones in Cluster 2. The IP addresses of these two Cisco IP Phones are 172.16.70.230 (directory number 1000) and 172.16.70.231 (directory number 1001), respectively.

Figure B-1 Sample Topology of Intra-Cluster Cisco IP Phone-to-Cisco IP Phone Calls



45436

Cisco IP Phone Initialization Process

The following procedure explains in detail the Cisco IP Phone initialization (or boot up) process.

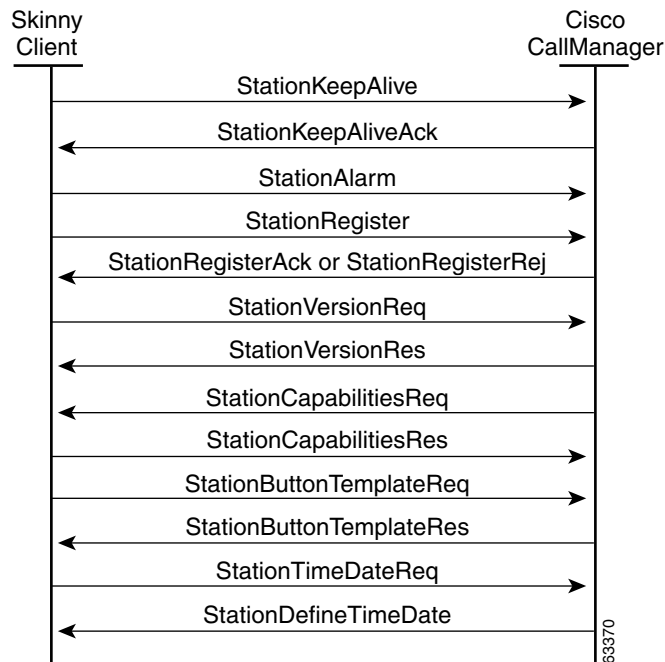
Procedure

- Step 1** If you have set the appropriate options in DHCP server (such as Option 066 or Option 150), the Cisco IP Phone sends a request, at initialization to the DHCP server to get an IP address, Domain Name System (DNS) server address, and TFTP server name or address. It also gets a default gateway address if you have set these options in the DHCP server (Option 003).
- Step 2** If a DNS name of the TFTP sever is sent by DHCP, you need a DNS server IP address to map the name to an IP address. Bypass this step if the DHCP server sends the IP address of the TFTP server. In this case study, the DHCP server sent the IP address of TFTP because DNS was not configured.
- Step 3** If a TFTP server name is not included in the DHCP reply, the Cisco IP Phone uses the default server name.
- Step 4** The configuration file (.cnf) file gets retrieved from the TFTP server. All .cnf files have the name SEP<mac_address>.cnf. If this is the first time the phone is registering with the Cisco CallManager, a default file, SEPdefault.cnf, gets downloaded to the Cisco IP Phone. In this case study, the first Cisco IP Phone uses the IP address 172.16.70.230 (its MAC address is SEP0010EB001720), and the second Cisco IP Phone uses the IP address 172.16.70.231 (its MAC address is SEP003094C26105).
- Step 5** All .cnf files include the IP address(es) for the primary and secondary Cisco CallManager(s). The Cisco IP Phone uses this IP address to contact the primary Cisco CallManager and to register.
- Step 6** Once the Cisco IP Phone connects and registers with Cisco CallManager, the Cisco CallManager tells the Cisco IP Phone which executable version (called a load ID) to run. If the specified version does not match the executing version on the Cisco IP Phone, the Cisco IP Phone will request the new executable from the TFTP server and reset automatically
-

Skinny Station Registration Process

Cisco IP Phones communicate with the Cisco CallManager by using the Cisco Skinny Station Protocol. The registration process allows a Skinny Station, such as the Cisco IP Phone, to inform the Cisco CallManager of its existence and to make calling possible. Figure B-2 provides a sample of this process.

Figure B-2 *Skinny Client Registration Sequence*



With the advent of the Cisco IP Phone 7960 and 7940 phone sets, the registration process increased in complexity. Figure B-3 illustrates the registration and initialization sequence for this telephone set.

Figure B-3 Cisco IP Phone 7960 or 7940 Registration and Initialization

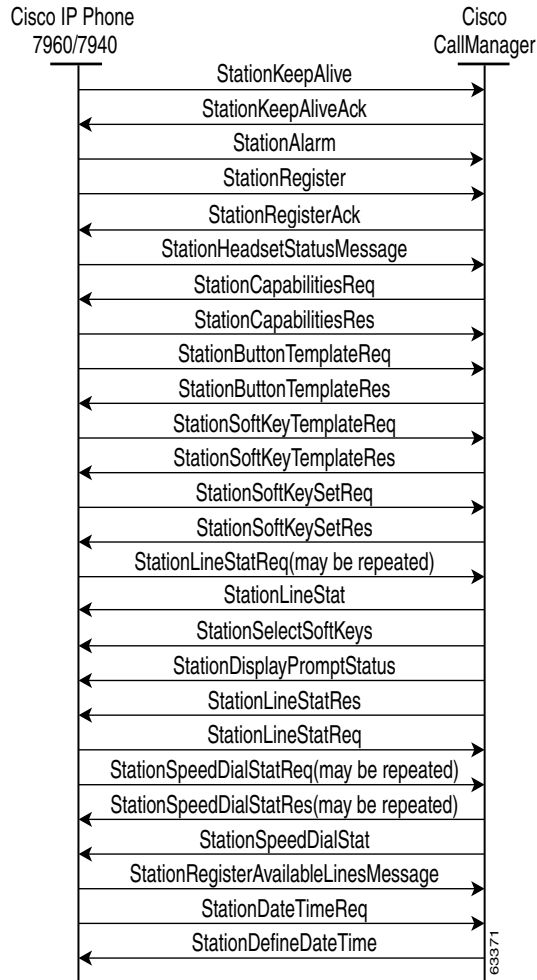


Table B-1 describes the primary messages in the Skinny Station registration process.

Table B-1 Skinny Station Registration Process Descriptions

Message	Description
Station Register	The station sends this message to announce its existence to the controlling Cisco CallManager.
Station Reset	Cisco CallManager sends this message to command the station to reset its processes.
Station IP Port	The station sends this message to provide Cisco CallManager with the User Datagram Protocol (UDP) port to be used with the Real-Time Protocol (RTP) stream.
Station Register Acknowledge	Cisco CallManager sends this message to acknowledge the registration of a station.
Station Register Reject	Cisco CallManager sends this message to reject a registration attempt from the indicated phone. char text [StationMaxDisplayTextSize]; }; Where: text represents a character string, maximum length of 33 bytes, containing a textual description of the reason that registration is rejected.
Station Capabilities Request	Cisco CallManager sends this message to request the current capabilities of the station. Station capabilities may include compression standard and other H.323 capabilities.
Station Version Request	The station sends this message to request the version number of the software load for the station.
Station Version Response	Cisco CallManager sends this message to inform the station of the appropriate software version number.

Table B-1 Skinny Station Registration Process Descriptions (continued)

Message	Description
Station Capabilities Response	The station sends this message to the Cisco CallManager in response to a Station Capabilities Request. The Cisco CallManager caches the station's capabilities and uses them to negotiate terminal capabilities with an H.323 compliant terminal.
Station Button Template Request	The station sends this message to request the button template definition for that specific terminal or Cisco IP Phone.
Station Button Template Response	Cisco CallManager sends this message to update the button template information that is contained in the station.
Station Time Date Request	The station sends this message to request the current date and time for internal usage and for displaying as a text string.
Station Define Time and Date	Cisco CallManager uses this message to provide the date and time information to the station. It provides time synchronization for the stations.

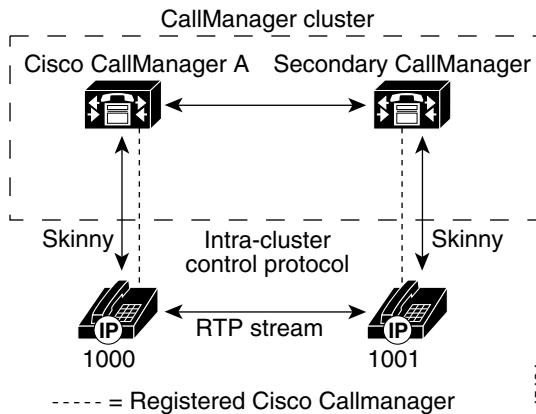
Cisco IP Phone-to-Cisco IP Phone Call Flow Within a Cluster

This section describes a Cisco IP Phone (directory number 1000) calling another Cisco IP Phone (directory number 1001) within the same cluster. The cluster represents a group of Cisco CallManagers having one common Publisher Structured Query Language (SQL) database and many Subscriber SQL databases.

In this cluster scenario, CCM1 identifies the publisher, and CCM2 identifies a subscriber. The two Cisco IP Phones (1000 and 1001) are registered to CCM1 and CCM2, respectively. The two Cisco CallManagers within a cluster communicate with each other using Intracluster Control Protocol (ICCP).

When a Cisco IP Phone goes off hook, it opens a control Skinny Station session (with TCP as the underlying protocol) with the Cisco CallManager. After call control signaling is established between the two Cisco IP Phones and their respective Cisco CallManagers, the RTP stream starts flowing directly between the two phones, as shown in Figure B-4. The next section provides an explanation of the Skinny Station call flow messages for this intracluster call.

Figure B-4 RTP Stream Between Phones 1000 and 1001



Cisco IP Phone-to-Cisco IP Phone Exchange of Skinny Station Messages During Call Flow

The Skinny Station, in this case a Cisco IP Phone, initiates a connection to the Cisco CallManager and then Cisco CallManager performs digit analysis before opening a control session with the destination Skinny Station.

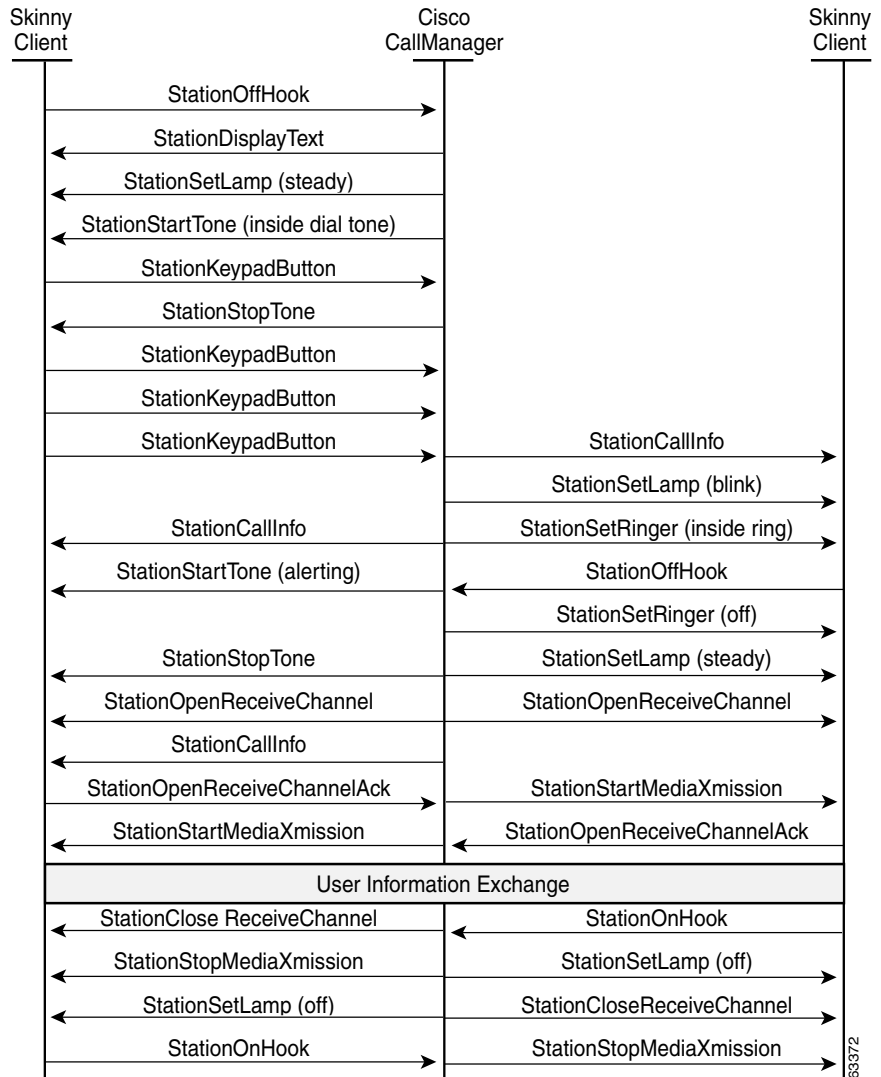


Note

The Skinny Station messages, written in English, can be understood by end users. Therefore, this section does not explain these messages. However, later sections explain the call flow Skinny Station messages when traces are being examined.

Figure B-5 shows a sample exchange of messages between two Skinny Clients.

Figure B-5 Skinny Client to Skinny Client Call Signaling



63372

Cisco CallManager Initialization Process

This section explains the initialization process of Cisco CallManager with the help of traces that are captured from CCM1 (identified by the IP address 172.16.70.228). As described previously, SDI traces provide a very effective troubleshooting tool because they detail every packet sent between endpoints.

This section describes the events that occur when Cisco CallManager is initialized. Understanding how to read traces will help you to properly troubleshoot the various Cisco CallManager processes and the effect of those processes on services such as conferencing and call forwarding.

The following messages from the Cisco CallManager SDI trace utility show the initialization process on one of the Cisco CallManagers, in this case, CCM1.

- The first message indicates that Cisco CallManager started its initialization process.
- The second message indicates that Cisco CallManager read the default database values (for this case, it is the primary or publisher database).
- The third message indicates Cisco CallManager received the various messages on TCP port 8002.
- The fourth message shows that, after receiving to these messages, Cisco CallManager added a second Cisco CallManager to its list: CCM2 (172.16.70.229).
- The fifth message indicates that Cisco CallManager has started and is running Cisco CallManager version 3.1(1).

```
16:02:47.765 CCM|CMPProcMon - CallManagerState Changed - Initialization
Started.
16:02:47.796 CCM|NodeId: 0, EventId: 107 EventClass: 3 EventInfo:
Cisco CM Database Defaults Read
16:02:49.937 CCM| SDL Info - NodeId: [1], Listen IP/Hostname:
[172.16.70.228], Listen Port: [8002]
16:02:49.984 CCM|dbProcs - Adding SdlLink to NodeId: [2], IP/Hostname:
[172.16.70.229]
16:02:51.031 CCM|NodeId: 1, EventId: 1 EventClass: 3 EventInfo:
Cisco CallManager Version=<3.1(1)> started
```

Self-Starting Processes

Once Cisco CallManager is up and running, it starts several other processes within itself. Some of these processes follow, including MulticastPoint Manager, UnicastBridge Manager, digit analysis, and route list. You will find the messages described during these processes very useful when you are troubleshooting a problem related to the features in Cisco CallManager.

For example, assume that the route lists are not functioning and are unusable. To troubleshoot this problem, you would monitor these traces to determine whether the Cisco CallManager has started RoutePlanManager and if it is trying to load the RouteLists. The sample configuration below shows that RouteListName="ipwan" and RouteGroupName="ipwan" are loading and starting.

```
16:02:51.031 CCM|MulticastPointManager - Started
16:02:51.031 CCM|UnicastBridgeManager - Started
16:02:51.031 CCM|MediaTerminationPointManager - Started
16:02:51.125 CCM|MediaCoordinator(1) - started
16:02:51.125 CCM|NodeId: 1, EventId: 1543 EventClass: 2 EventInfo:
Database manager started
16:02:51.234 CCM|NodeId: 1, EventId: 1542 EventClass: 2 EventInfo:
Link manager started
16:02:51.390 CCM|NodeId: 1, EventId: 1541 EventClass: 2 EventInfo:
Digit analysis started
16:02:51.406 CCM|RoutePlanManager - Started, loading RouteLists
16:02:51.562 CCM|RoutePlanManager - finished loading RouteLists
16:02:51.671 CCM|RoutePlanManager - finished loading RouteGroups
16:02:51.671 CCM|RoutePlanManager - Displaying Resulting RoutePlan
16:02:51.671 CCM|RoutePlanServer - RouteList Info, by RouteList and
RouteGroup Selection Order
16:02:51.671 CCM|RouteList - RouteListName='ipwan'
16:02:51.671 CCM|RouteList - RouteGroupName='ipwan'
16:02:51.671 CCM|RoutePlanServer - RouteGroup Info, by RouteGroup and
Device Selection Order
16:02:51.671 CCM|RouteGroup - RouteGroupName='ipwan'
```

The following trace shows the RouteGroup adding the device 172.16.70.245, which is CCM3 located in Cluster 1 and is considered an H.323 device. In this case, the RouteGroup is created to route calls to CCM3 in Cluster 1 with Cisco IOS Gatekeeper permission. If a problem occurs while routing the call to a Cisco IP Phone located in Cluster 1, the following messages would help you find the cause of the problem.

```
16:02:51.671 CCM|RouteGroup - DeviceName='172.16.70.245'
16:02:51.671 CCM|RouteGroup -AllPorts
```

Part of the initialization process shows that Cisco CallManager is adding "Dns" (Directory Numbers). By reviewing these messages, you can determine whether the Cisco CallManager has read the directory number from the database.

```
16:02:51.671 CCM|NodeId: 1, EventId: 1540 EventClass: 2 EventInfo:
Call control started
16:02:51.843 CCM|ProcessDb - Dn = 2XXX, Line = 0,
Display = , RouteThisPattern, NetworkLocation = OffNet,
DigitDiscardingInstruction = 1, WhereClause =
16:02:51.859 CCM|Digit analysis: Add local pattern 2XXX , PID: 1,80,1
16:02:51.859 CCM|ForwardManager - Started
16:02:51.984 CCM|CallParkManager - Started
16:02:52.046 CCM|ConferenceManager - Started
```

In the following traces, the Device Manager in Cisco CallManager statically initializes two devices. The device with IP address 172.17.70.226 represents a gatekeeper, and the device with IP address 172.17.70.245 gets another Cisco CallManager in a different cluster. That Cisco CallManager gets registered as an H.323 Gateway with this Cisco CallManager.

```
16:02:52.250 CCM|DeviceManager: Statically Initializing Device;
DeviceName=172.16.70.226
16:02:52.250 CCM|DeviceManager: Statically Initializing Device;
DeviceName=172.16.70.245
```

Cisco CallManager Registration Process

Another important part of the SDI trace involves the registration process. When a device is powered up, it gets information via DHCP, connects to the TFTP server for its .cnf file, and then connects to the Cisco CallManager that is specified in the .cnf file. The device could be an MGCP gateway, a Skinny gateway, or a Cisco IP Phone. Therefore, you need to be able to discover whether devices have successfully registered on the Cisco AVVID network.

In the following trace, Cisco CallManager has received new connections for registration. The registering devices are MTP_nsa-cm1 (MTP services on CCM1), and CFB_nsa-cm1 (Conference Bridge service on CCM1). Although these are software services that are running on Cisco CallManager, they get treated internally as different external services and therefore get assigned a TCPHandle, socket number, and port number as well as a device name.

```
16:02:52.750 CCM|StationInit - New connection accepted. DeviceName=,
TCPHandle=0x4fbaa00, Socket=0x594, IPAddr=172.16.70.228, Port=3279,
StationD=[0,0,0]
16:02:52.750 CCM|StationInit - New connection accepted. DeviceName=,
TCPHandle=0x4fe05e8, Socket=0x59c, IPAddr=172.16.70.228, Port=3280,
StationD=[0,0,0]
16:02:52.781 CCM|StationInit - Processing StationReg. regCount: 1
DeviceName=MTP_nsa-cml, TCPHandle=0x4fbaa00, Socket=0x594,
IPAddr=172.16.70.228, Port=3279, StationD=[1,45,2]
16:02:52.781 CCM|StationInit - Processing StationReg. regCount: 1
DeviceName=CFB_nsa-cml, TCPHandle=0x4fe05e8, Socket=0x59c,
IPAddr=172.16.70.228, Port=3280, StationD=[1,96,2]
```

In the following trace, Skinny Station messages get sent between a Cisco IP Phone and Cisco CallManager. The Cisco IP Phone (172.16.70.231) is registering with Cisco CallManager. Table B-1 provides the descriptions of Skinny Station messages. As soon as Cisco CallManager receives the registration request from a Cisco IP Phone, it assigns a TCPHandle number to this device. This number remains the same until the device or Cisco CallManager is restarted. Therefore, you can follow all the events related to a particular device by searching for or keeping track of the device TCPHandle number, which appears in hexadecimal notation. Also, notice that Cisco CallManager provides the load ID to the Cisco IP Phone. Based on this load ID, the Cisco IP Phone runs the executable file (acquired from the TFTP server) that corresponds to the device.

```
16:02:57.000 CCM|StationInit - New connection accepted. DeviceName=,
TCPHandle=0x4fbbc30, Socket=0x5a4, IPAddr=172.16.70.231, Port=52095,
StationD=[0,0,0]
16:02:57.046 CCM|NodeId: 1, EventId: 1703 EventClass: 2 EventInfo:
Station Alarm, TCP Handle: 4fbbc30, Text: Name=SEP003094C26105
Load=AJ.30 Params=Status/IPAddr LastTime=A P1: 2304(900) P2:
-414838612 (e74610ac)
16:02:57.046 CCM|StationInit - ***** InboundStim - AlarmMessageID
tcpHandle=0x4fbbc30 Message="Name=SEP003094C26105 Load=AJ.30
Params=Status/IPAddr LastTime=A" Parm1=2304 (900) Parm2=-414838612
(e74610ac)
16:02:57.093 CCM|StationInit - Processing StationReg. regCount: 1
DeviceName=SEP003094C26105, TCPHandle=0x4fbbc30, Socket=0x5a4,
IPAddr=172.16.70.231, Port=52095, StationD=[1,85,1]
16:02:57.093 CCM|StationInit - InboundStim - IpPortMessageID:
32715(0x7fcb) tcpHandle=0x4fbbc30
```

Cisco CallManager KeepAlive Process

The station, device, or service and the Cisco CallManager use the following messages to maintain a knowledge of the communications channel between them. The messages begin the KeepAlive sequence that ensures that the communications link between the Cisco CallManager and the station remains active. The following messages can originate from either the Cisco CallManager or the station.

```
16:03:02.328 CCM|StationInit - InboundStim - KeepAliveMessage -
Forward KeepAlive to StationD. DeviceName=MTP_nsa-cm2,
TCPHandle=0x4fa7dc0, Socket=0x568, IPAddr=172.16.70.229, Port=1556,
StationD=[1,45,1]
16:03:02.328 CCM|StationInit - InboundStim - KeepAliveMessage -
Forward KeepAlive to StationD. DeviceName=CFB_nsa-cm2,
TCPHandle=0x4bf8a70, Socket=0x57c, IPAddr=172.16.70.229, Port=1557,
StationD=[1,96,1]
16:03:06.640 CCM|StationInit - InboundStim - KeepAliveMessage -
Forward KeepAlive to StationD. DeviceName=SEP0010EB001720,
TCPHandle=0x4fbb150, Socket=0x600, IPAddr=172.16.70.230, Port=49211,
StationD=[1,85,2]
16:03:06.703 CCM|StationInit - InboundStim - KeepAliveMessage -
Forward KeepAlive to StationD. DeviceName=SEP003094C26105,
TCPHandle=0x4fbbc30, Socket=0x5a4, IPAddr=172.16.70.231, Port=52095,
StationD=[1,85,1]
```

The messages in the following trace depict the KeepAlive sequence that indicates that the communications link between the Cisco CallManager and the station is active. Again, these messages can originate from either the Cisco CallManager or the station.

```
16:03:02.328 CCM|MediaTerminationPointControl -
stationOutputKeepAliveAck tcpHandle=4fa7dc0
16:03:02.328 CCM|UnicastBridgeControl - stationOutputKeepAliveAck
tcpHandle=4bf8a70
16:03:06.703 CCM|StationInit - InboundStim - IpPortMessageID:
32715(0x7fcb) tcpHandle=0x4fbbc30
16:03:06.703 CCM|StationD - stationOutputKeepAliveAck
tcpHandle=0x4fbbc30
```

Cisco CallManager Intracluster Call Flow Traces

The following SDI traces explore the intracluster call flow in detail. You can identify the Cisco IP Phones in the call flow by the directory number (dn), tcpHandle, and IP address. A Cisco IP Phone (dn: 1001, tcpHandle: 0x4fbbc30, IP address: 172.16.70.231) located in Cluster 2 is calling another Cisco IP Phone in the same Cluster (dn=1000, tcpHandle= 0x4fbb150, IP address= 172.16.70.230). Remember that you can follow a device through the trace by looking at the TCP handle value, time stamp, or name of the device. The TCP handle value for the device remains the same until the device is rebooted or goes offline.

The following traces show that the Cisco IP Phone (1001) has gone off hook. The trace below shows the unique messages, TCP handle, and the called number, which display on the Cisco IP Phone. No calling number appears at this point because the user has not tried to dial any digits. The information below appears in the form of Skinny Station messages between the Cisco IP Phones and the Cisco CallManager.

```
16:05:41.625 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x4fbbc30
16:05:41.625 CCM|StationD - stationOutputDisplayText
tcpHandle=0x4fbbc30, Display= 1001
```

The next trace shows Skinny Station messages going from Cisco CallManager to a Cisco IP Phone. The first message is to turn on the lamp on the calling party Cisco IP Phone.

```
16:05:41.625 CCM|StationD - stationOutputSetLamp stim: 9=Line
instance=1 lampMode=LampOn tcpHandle=0x4fbbc30
```

Cisco CallManager uses the stationOutputCallState message to notify the station of certain call-related information.

```
16:05:41.625 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
```

Cisco CallManager uses the stationOutputDisplayPromptStatus message to cause a call-related prompt message to display on the Cisco IP Phone.

```
16:05:41.625 CCM|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x4fbbc30
```

Cisco CallManager uses the stationOutputSelectSoftKey message to cause the Skinny Station to choose a specific set of soft keys.

```
16:05:41.625 CCM|StationD - stationOutputSelectSoftKeys
tcpHandle=0x4fbbc30
```

Cisco CallManager uses the next message to instruct the Skinny Station as to the correct line context for the display.

```
16:05:41.625 CCM|StationD - stationOutputActivateCallPlane
tcpHandle=0x4fbbc30
```

In the following message, the digit analysis process is ready to identify incoming digits and check them for potential routing matches in the database. The entry, `cn=1001`, represents the calling party number where `dd=""` represents the dialed digit, which would show the called part number. The phone sends `StationInit` messages, Cisco CallManager sends `StationD` messages, and Cisco CallManager performs digit analysis.

```
16:05:41.625 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="")
16:05:41.625 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
```

The following debug message shows that the Cisco CallManager is providing inside dial tone to the calling party Cisco IP Phone.

```
16:05:41.625 CCM|StationD - stationOutputStartTone: 33=InsideDialTone
tcpHandle=0x4fbbc30
```

After Cisco CallManager detects an incoming message and recognizes that the keypad button **1** has been pressed on the Cisco IP Phone, it immediately stops the output tone.

```
16:05:42.890 CCM|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 1 tcpHandle=0x4fbbc30
16:05:42.890 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
16:05:42.890 CCM|StationD - stationOutputSelectSoftKeys
tcpHandle=0x4fbbc30
16:05:42.890 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="1")
16:05:42.890 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
16:05:43.203 CCM|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x4fbbc30
16:05:43.203 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="10")
16:05:43.203 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
16:05:43.406 CCM|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x4fbbc30
```

```

16:05:43.406 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="100")
16:05:43.406 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
16:05:43.562 CCM|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x4fbbc30
16:05:43.562 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="1000")

```

After the Cisco CallManager has received enough digits to match, it provides the digit analysis results in a table format. Cisco CallManager ignores any extra digits that are pressed on the phone after this point because a match has already been found.

```

16:05:43.562 CCM|Digit analysis: analysis results
16:05:43.562 CCM| |PretransformCallingPartyNumber=1001
|CallingPartyNumber=1001
|DialingPattern=1000
|DialingRoutePatternRegularExpression=(1000)
|PotentialMatches=PotentialMatchesExist
|DialingSdlProcessId=(1,38,2)
|PretransformDigitString=1000
|PretransformPositionalMatchList=1000
|CollectedDigits=1000
|PositionalMatchList=1000
|RouteBlockFlag=RouteThisPattern

```

The next trace shows that Cisco CallManager is sending out this information to a called party phone (the tcpHandle number identifies the phone).

```

16:05:43.578 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001, CallingParty=1001, CalledPartyName=1000,
CalledParty=1000, tcpHandle=0x4fbb150

```

The next trace indicates that Cisco CallManager is ordering the lamp to blink for incoming call indication on the called party Cisco IP Phone.

```

16:05:43.578 CCM|StationD - stationOutputSetLamp stim: 9=Line
instance=1 lampMode=LampBlink tcpHandle=0x4fbb150

```

In the following traces, Cisco CallManager provides ringer, display notification, and other call-related information to the called party Cisco IP Phone. Again, you can see that all messages get directed to the same Cisco IP Phone because the same tcpHandle gets used throughout the traces.

```

16:05:43.578 CCM|StationD - stationOutputSetRinger: 2=InsideRing
tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputDisplayNotify
tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputSelectSoftKeys
tcpHandle=0x4fbb150

```

Notice that Cisco CallManager also provides similar information to the calling party Cisco IP Phone. Again, the tcpHandle differentiates between Cisco IP Phones.

```

16:05:43.578 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001, CallingParty=1001, CalledPartyName=,
CalledParty=1000, tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001, CallingParty=1001, CalledPartyName=1000,
CalledParty=1000, tcpHandle=0x4fbbc30

```

In the next trace, Cisco CallManager provides an alerting or ringing tone to the calling party Cisco IP Phone, notifying that the connection has been established.

```

16:05:43.578 CCM|StationD - stationOutputStartTone: 36=AlertingTone
tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputSelectSoftKeys
tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x4fbbc30

```

At this point, the called party's Cisco IP Phone goes off hook; therefore, Cisco CallManager stops generating the ringer tone to calling party.

```

16:05:45.140 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30

```

In the following messages, Cisco CallManager causes the Skinny Station to begin receiving a Unicast RTP stream. To do so, Cisco CallManager provides the IP address of the called party as well as codec information and packet size in msec (milliseconds). PacketSize designates an integer that contains the sampling time, in milliseconds, that is used to create the RTP packets.


Note

Normally this value gets set to 30 msec. In this case, it is set to 20 msec.

```
16:05:45.140 CCM|StationD - stationOutputOpenReceiveChannel
tcpHandle=0x4fbbc30 myIP: e74610ac (172.16.70.231)
16:05:45.140 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
```

Similarly, Cisco CallManager provides information to the called party (1000).

```
16:05:45.140 CCM|StationD - stationOutputOpenReceiveChannel
tcpHandle=0x4fbb150 myIP: e64610ac (172.16.70.230)
16:05:45.140 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
```

Cisco CallManager has received the acknowledgment message from called party for establishing the open channel for RTP stream, as well as the IP address of the called party. This message informs the Cisco CallManager of two pieces of information about the Skinny Station. First, it contains the status of the open action. Second, it contains the receive port address and number for transmission to the remote end. The IP address of the transmitter (calling part) of the RTP stream is ipAddr, and PortNumber is the IP port number of the RTP stream transmitter (calling party).

```
16:05:45.265 CCM|StationInit - InboundStim -
StationOpenReceiveChannelAckID tcpHandle=0x4fbb150, Status=0,
IpAddr=0xe64610ac, Port=17054, PartyID=2
```

Cisco CallManager uses the following messages to order the station to begin transmitting the audio stream to the indicated remote Cisco IP Phone IP address and port number.

```
16:05:45.265 CCM|StationD - stationOutputStartMediaTransmission
tcpHandle=0x4fbbc30 myIP: e74610ac (172.16.70.231)
16:05:45.265 CCM|StationD - RemoteIpAddr: e64610ac (172.16.70.230)
RemoteRtpPortNumber: 17054 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
```

In the following traces, the previously explained messages are sent to the called party. The messages that indicate that the RTP media stream has been started between the called and calling party, follow these messages.

```
16:05:45.312 CCM|StationD - stationOutputStartMediaTransmission
tcpHandle=0x4fbb150 myIP: e64610ac (172.16.70.230)
16:05:45.328 CCM|StationD - RemoteIpAddr: e74610ac (172.16.70.231)
RemoteRtpPortNumber: 18448 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
16:05:46.203 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x4fbbc30
```

The calling party Cisco IP Phone finally goes on hook, which terminates all the control messages between the Skinny Station and Cisco CallManager as well as the RTP stream between Skinny Stations.

```
16:05:46.203 CCM|StationInit - InboundStim - OnHookMessageID  
tcpHandle=0x4fbbc30
```



Case Study: Troubleshooting Cisco IP Phone-to-Cisco IOS Gateway Calls

The case study described in Appendix A, “Opening a Case With TAC,” described the call flow for an intracluster call. The case study in this appendix examines a Cisco IP Phone that is calling through a Cisco IOS Gateway to a phone that is connected through a local PBX or on the Public Switched Telephone Network (PSTN). Conceptually, when the call reaches the Cisco IOS Gateway, the gateway will forward the call to either a phone connected to an FXS port or to the PBX. If the call is forwarded to the PBX, it could terminate to a phone that is connected to a local PBX, or the PBX forwards it over the PSTN, and the call will terminate somewhere on the PSTN.

This appendix contains the following topics:

- Call Flow Traces
- Debug Messages and Show Commands on the Cisco IOS Gatekeeper
- Debug Messages and Show Commands on the Cisco IOS Gateway
- Cisco IOS Gateway with T1/PRI Interface
- Cisco IOS Gateway with T1/CAS Interface

Call Flow Traces

This section discusses call flow through examples from the Cisco CallManager trace file CCM000000000. The traces in this case study focus only on the call flow itself because Appendix A, “Opening a Case With TAC” (for example, initialization, registration, and KeepAlive mechanism) already explained the more detailed trace information.

In this call flow, a Cisco IP Phone (directory number 1001) that is located in cluster 2 is calling a phone (directory number 3333) that is located somewhere on the PSTN. Remember that you can follow a device through the trace by looking at the TCP handle value, time stamp, or name of the device. The TCP handle value for the device remains the same until the device is rebooted or goes off line.

In the following traces, the Cisco IP Phone (1001) has gone off hook. The trace shows the unique messages, TCP handle, and the calling number, which displays on the Cisco IP Phone. No called number appears at this point, because the user has not tried to dial any digits.

```
16:05:46.37515:20:18.390 CCM|StationInit - InboundStim -
OffHookMessageID tcpHandle=0x5138d98
```

```
15:20:18.390 CCM|StationD - stationOutputDisplayText
tcpHandle=0x5138d98, Display=1001
```

In the following traces, the user is dialing the DN 3333, one digit at a time. The number 3333 specifies the destination number of the phone, which is located somewhere on the PSTN network. The digit analysis process of the Cisco CallManager is currently active and is analyzing the digits to discover where the call needs to get routed. Appendix A, “Opening a Case With TAC” provides a more detailed explanation of the digit analysis

```
15:20:18.390 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="")
15:20:19.703 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="3")
15:20:20.078 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="33")
15:20:20.718 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="333")
15:20:21.421 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="3333")
15:20:21.421 CCM|Digit analysis: analysis results
```

In the following traces, the digit analysis has completed, calling and called party are matched, and the information has been parsed.

```
|CallingPartyNumber=1001
|DialingPattern=3333
|DialingRoutePatternRegularExpression=(3333)
|PretransformDigitString=3333
|PretransformPositionalMatchList=3333
|CollectedDigits=3333
|PositionalMatchList=3333
```

In the following traces, the number 0 indicates the originating location, and the number 1 indicates the destination location. BW = -1 determines the bandwidth of the originating location. The value -1 implies that the bandwidth is infinite. The bandwidth is infinite because the call originated from a Cisco IP Phone located in a LAN environment. BW = 64 determines the bandwidth of the destination location. The call destination specifies a phone located in a PSTN, and the codec type that is used is G.711 (64 Kbps).

```
15:20:21.421 CCM|Locations:Orig=0 BW=-1 Dest=1 BW=64 (-1 implies
infinite bw available)
```

The following traces show the calling and called party information. In this example, the calling party name and number are the same because the administrator has not configured a display name, such as John Smith.

```
15:20:21.421 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001, CallingParty=1001, CalledPartyName=,
CalledParty=3333, tcpHandle=0x5138d98
```

The following trace shows that the H.323 code has been initialized and is sending an H.225 setup message. You can also see the traditional HDLC SAPI messages, the IP address of the called side in hexadecimal, and the port numbers.

```
15:20:21.421 CCM|Out Message -- H225SetupMsg -- Protocol= H225Protocol
15:20:21.421 CCM|MMan_Id= 1. (iep= 0 dsl= 0 sapi= 0 ces= 0
IpAddr=e24610ac IpPort=47110)
```

The following trace shows the calling and called party information as well as the H.225 alerting message. Also shown is the mapping of a Cisco IP Phone hexadecimal value to the IP address. The IP address of the Cisco IP Phone (1001) is 172.16.70.231.

```
15:20:21.437 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001, CallingParty=1001, CalledPartyName=,
CalledParty=3333, tcpHandle=0x5138d98
15:20:21.453 CCM|In Message -- H225AlertMsg -- Protocol= H225Protocol
```

```
15:20:21.953 CCM|StationD - stationOutputOpenReceiveChannel
tcpHandle=0x5138d98 myIP: e74610ac (172.16.70.231)
```

The following trace shows the compression type that is used for this call (G.711 mu-law).

```
15:20:21.953 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
```

After the H.225 alert message has been sent, H.323 initializes H.245. The following trace shows the calling and called party information, and the H.245 messages. Notice that the TCP handle value remains the same as before, indicating that this is the continuation of the same call.

```
15:20:22.062 CCM|H245Interface(3) paths established ip = e74610ac,
port = 23752
15:20:22.062 CCM|H245Interface(3) OLC outgoing confirm ip = e24610ac,
port = 16758
15:20:22.062 CCM|MediaManager - wait_AuConnectInfo - received
response, forwarding
```

The following trace shows the H.225 connection message, as well as other information. When the H.225 connection message is received, the call connected.

```
15:20:22.968 CCM|In Message -- H225ConnectMsg -- Protocol=
H225Protocol
15:20:22.968 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001, CallingParty=1001, CalledPartyName=,
CalledParty=3333, tcpHandle=0x5138d98
15:20:22.062 CCM|MediaCoordinator - wait_AuConnectInfoInd
15:20:22.062 CCM|StationD - stationOutputStartMediaTransmission
tcpHandle=0x5138d98 myIP: e74610ac (172.16.70.231)
15:20:22.062 CCM|StationD - RemoteIpAddr: e24610ac (172.16.70.226)
RemoteRtpPortNumber: 16758 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
15:20:22.062 CCM|Locations:Orig=0 BW=-1Dest=1 BW=6(-1 implies infinite
bw available)
```

The following message shows that an on-hook message from the Cisco IP Phone (1001) is being received. As soon as an on-hook message is received, the H.225 and Skinny Station device disconnection messages are sent, and the entire H.225 message is seen. This final message indicates that the call terminated.

```
15:20:27.296 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x5138d98
15:20:27.296 CCM|ConnectionManager -wait_AuDisconnectRequest
(16777247,16777248): STOP SESSION
```

```
15:20:27.296 CCM|MediaManager - wait_AuDisconnectRequest - StopSession
sending disconnect to (64,5) and remove connection from list
15:20:27.296 CCM| Device SEP003094C26105 , UnRegisters with SDL Link
to monitor NodeID= 1
15:20:27.296 CCM|StationD - stationOutputCloseReceiveChannel
tcpHandle=0x5138d98 myIP: e74610ac (172.16.70.231)
15:20:27.296 CCM|StationD - stationOutputStopMediaTransmission
tcpHandle=0x5138d98 myIP: e74610ac (172.16.70.231)
15:20:28.328 CCM|In Message -- H225ReleaseCompleteMsg -- Protocol=
H225Protocol
```

Debug Messages and Show Commands on the Cisco IOS Gatekeeper

In the Call Flow Traces discussion covers the Cisco CallManager SDI trace in detail. In the topology for this case study, the debug ras command has been turned on in the Cisco IOS Gatekeeper.

The following debug messages show that the Cisco IOS Gatekeeper is receiving the admission request (ARQ) for the Cisco CallManager (172.16.70.228), followed by other successful Remote Access Server (RAS) messages. Finally, the Cisco IOS Gatekeeper sends an admission confirmed (ACF) message to the Cisco CallManager.

```
*Mar 12 04:03:57.181: RASLibRASRecvData ARQ (seq# 3365) rcvd from
[172.16.70.228883] on sock [0x60AF038C]
*Mar 12 04:03:57.181: RASLibRAS_WK_TInit ipsock [0x60A7A68C] setup
successful
*Mar 12 04:03:57.181: RASLibRAS_sendto msg length 16 from
172.16.70.2251719 to 172.16.70.228883
*Mar 12 04:03:57.181: RASLibRASSendACF ACF (seq# 3365) sent to
172.16.70.228
```

The following debug messages show that the call is in progress.

```
*Mar 12 04:03:57.181: RASLibRASRecvData successfully rcvd message of
length 55 from 172.16.70.228883
```

The following debug messages show that the Cisco IOS Gatekeeper has received a disengaged request (DRQ) from the Cisco CallManager (172.16.70.228), and the Cisco IOS Gatekeeper has sent a disengage confirmed (DCF) to the Cisco CallManager.

```
*Mar 12 04:03:57.181: RASLibRASRecvData DRQ (seq# 3366) rcvd from
[172.16.70.228883] on sock [0x60AF038C]
*Mar 12 04:03:57.181: RASLibRAS_sendto msg length 3 from
172.16.70.2251719 to 172.16.70.228883
*Mar 12 04:03:57.181: RASLibRASsendDCF DCF (seq# 3366) sent to
172.16.70.228
*Mar 12 04:03:57.181: RASLibRASRecvData successfully rcvd message of
length 124 from 172.16.70.228883
```

The command `show gatekeeper endpoints` on the Cisco IOS Gatekeeper shows that all four Cisco CallManagers are registered with the Cisco IOS Gatekeeper. Remember that in the topology for this case study, four Cisco CallManagers exist, two in each cluster. This Cisco IOS Gatekeeper includes two zones and each zone includes two Cisco CallManagers.

R2514-1#show gatekeeper endpoints

```

                                GATEKEEPER ENDPOINT REGISTRATION
                                =====
CallSignalAddr  Port  RASignalAddr  Port  Zone Name          Type
-----
172.16.70.228   2     172.16.70.228   1493  gka.cisco.com
VOIP-GW
H323-ID: ac1046e4->ac1046f5
172.16.70.229   2     172.16.70.229   3923  gka.cisco.com
VOIP-GW
H323-ID: ac1046e5->ac1046f5
172.16.70.245   1     172.16.70.245   1041  gkb.cisco.com
VOIP-GW
H323-ID: ac1046f5->ac1046e4
172.16.70.243   1     172.16.70.243   2043  gkb.cisco.com
VOIP-GW
H323-ID: ac1046f5->ac1046e4
Total number of active registrations = 4
```

Debug Messages and Show Commands on the Cisco IOS Gateway

Debug Messages and Show Commands on the Cisco IOS Gatekeeper, the Cisco IOS Gatekeeper show commands and debug outputs discusses in detail. This section focuses on the debug output and show commands on the Cisco IOS Gateway. In the topology for this case study, calls go through the

Cisco IOS Gateways. The Cisco IOS Gateway interfaces to the PSTN or PBX with either T1/CAS or T1/PRI interfaces. The following example shows debug output of commands such as debug voip ccapi inout, debug H225 events, and debug H225 asn1.

In the following debug output, the Cisco IOS Gateway accepts the TCP connection request from Cisco CallManager (172.16.70.228) on port 2328 for H.225.

```
*Mar 12 04:03:57.169: H225Lib::h225TAccept: TCP connection accepted
from 172.16.70.228:2328 on socket [1]
*Mar 12 04:03:57.169: H225Lib::h225TAccept: Q.931 Call State is
initialized to be [Null].
*Mar 12 04:03:57.177: Hex representation of the received
TPKTO3000065080000100
```

The following debug output shows that the H.225 data is coming from the Cisco CallManager on this TCP session. Notice the protocolIdentifier, which indicates the H.323 version being used, in this debug output. The following debug shows that H.323 version 2 is being used. The example also shows the called and calling party numbers.

```
- Source Address H323-ID
- Destination Address e164
*Mar 12 04:03:57.177: H225Lib::h225RecvData: Q.931 SETUP
received from socket [1]value H323-UserInformation ::=
*Mar 12 04:03:57.181: {
*Mar 12 04:03:57.181:   h323-uu-pdu
*Mar 12 04:03:57.181:   {
*Mar 12 04:03:57.181:     h323-message-body setup :
*Mar 12 04:03:57.181:     {
*Mar 12 04:03:57.181:       protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:57.181:       sourceAddress
*Mar 12 04:03:57.181:       {
*Mar 12 04:03:57.181:         h323-ID : "1001"
*Mar 12 04:03:57.181:       },
*Mar 12 04:03:57.185:       destinationAddress
*Mar 12 04:03:57.185:       {
*Mar 12 04:03:57.185:         e164 : "3333"
*Mar 12 04:03:57.185:       },
*Mar 12 04:03:57.189:     H225Lib::h225RecvData: State changed to
[Call Present].
```

The following debug output shows Call Control Application Programming Interface (CCAPi). Call Control APi indicates an incoming call. You can also see called and calling party information in the following output. CCAPi matches the

dial peer 0, which is the default dial peer. It matches dial peer 0 because the CCAPi could not find any other dial peer for the calling number, so it is using the default dial peer.

```
*Mar 12 04:03:57.189: cc_api_call_setup_ind (vdbPtr=0x616C9F54,
callInfo={called=3333, calling=1001, fdest=1 peer_tag=0},
callID=0x616C4838)
*Mar 12 04:03:57.193: cc_process_call_setup_ind (event=0x617A2B18)
handed call to app "SESSION"
*Mar 12 04:03:57.193: sess_appl: ev(19=CC_EV_CALL_SETUP_IND), cid(17),
disp(0)
*Mar 12 04:03:57.193: ccCallSetContext (callID=0x11,
context=0x61782BBC)
Mar 12 04:03:57.193: ssaCallSetupInd finalDest cllng(1001),
clled(3333)
*Mar 12 04:03:57.193: ssaSetupPeer cid(17) peer list: tag(1)
*Mar 12 04:03:57.193: ssaSetupPeer cid(17), destPat(3333), matched(4),
prefix(), peer(6179E63C)
*Mar 12 04:03:57.193: ccCallSetupRequest (peer=0x6179E63C, dest=,
params=0x61782BD0 mode=0, *callID=0x617A87C0)
*Mar 12 04:03:57.193: callingNumber=1001, calledNumber=3333,
redirectNumber=
*Mar 12 04:03:57.193: accountNumber=,finalDestFlag=1,
guid=0098.89c8.9233.511d.0300.cddd.ac10.46e6
```

The CCAPi matches the dial-peer 1 with the destination pattern, which is the called number 3333. Keep in mind that peer_tag means dial peer. Notice the calling and called party number in the request packet.

```
*Mar 12 04:03:57.193: peer_tag=1
*Mar 12 04:03:57.197: ccIFCallSetupRequest: (vdbPtr=0x617BE064, dest=,
callParams={called=3333, calling=1001, fdest=1, voice_peer_tag=1},
mode=0x0)
```

The following debug output shows that the H.225 alerting messages are returning to the Cisco CallManager.

```
*Mar 12 04:03:57.197: ccCallSetContext (callID=0x12,
context=0x61466B30)
*Mar 12 04:03:57.197: ccCallProceeding (callID=0x11, prog_ind=0x0)
*Mar 12 04:03:57.197: cc_api_call_proceeding(vdbPtr=0x617BE064,
callID=0x12, prog_ind=0x0)
*Mar 12 04:03:57.197: cc_api_call_alert(vdbPtr=0x617BE064,
callID=0x12, prog_ind=0x8, sig_ind=0x1)
*Mar 12 04:03:57.201: sess_appl: ev(17=CC_EV_CALL_PROCEEDING),
cid(18), disp(0)
```

```

*Mar 12 04:03:57.201: ssa:
cid(18)st(1)oldst(0)cfid(-1)csize(0)in(0)fDest(0)-cid2(17)st2(1)oldst2
(0)
*Mar 12 04:03:57.201: ssaIgnore cid(18), st(1),oldst(1), ev(17)
*Mar 12 04:03:57.201: sess_appl: ev(7=CC_EV_CALL_ALERT), cid(18),
disp(0)
*Mar 12 04:03:57.201: ssa:
cid(18)st(1)oldst(1)cfid(-1)csize(0)in(0)fDest(0)-cid2(17)st2(1)oldst2
(0)
*Mar 12 04:03:57.201: ssaFlushPeerTagQueue cid(17) peer list: (empty)
*Mar 12 04:03:57.201: ccCallAlert (callID=0x11, prog_ind=0x8,
sig_ind=0x1)
*Mar 12 04:03:57.201: ccConferenceCreate (confID=0x617A8808,
callID1=0x11, callID2=0x12, tag=0x0)
*Mar 12 04:03:57.201: cc_api_bridge_done (confID=0x7,
srcIF=0x616C9F54, srcCallID=0x11, dstCallID=0x12, disposition=0,
tag=0x0)value H323-UserInformation
*Mar 12 04:03:57.201: {
*Mar 12 04:03:57.201:   h323-uu-pdu
*Mar 12 04:03:57.201:   {
*Mar 12 04:03:57.201:     h323-message-body alerting :
*Mar 12 04:03:57.201:     {
*Mar 12 04:03:57.201:       protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:57.205:       destinationInfo
*Mar 12 04:03:57.205:       {
*Mar 12 04:03:57.205:         mc FALSE,
*Mar 12 04:03:57.205:         undefinedNode FALSE
*Mar 12 04:03:57.205:       },

```

Notice in this packet that Cisco IOS is also sending the H.245 address and port number to Cisco CallManager. Sometimes the Cisco IOS Gateway will send the unreachable address, which could cause either no audio or one-way audio.

```

*Mar 12 04:03:57.205:           h245Address ipAddress :
*Mar 12 04:03:57.205:           {
*Mar 12 04:03:57.205:             ip 'AC1046E2'H,
*Mar 12 04:03:57.205:             port 011008
*Mar 12 04:03:57.205:           },
*Mar 12 04:03:57.213: Hex representation of the ALERTING TPKT to
send.0300003D0100
*Mar 12 04:03:57.213:
*Mar 12 04:03:57.213:           H225Lib::h225AlertRequest: Q.931 ALERTING
sent from socket [1]. Call state changed to [Call Received].
*Mar 12 04:03:57.213: cc_api_bridge_done (confID=0x7,
srcIF=0x617BE064, srcCallID=0x12, dstCallID=0x11, disposition=0,
tag=0x0)

```

The following debug output shows that the H.245 session is coming up. You can see the capability indication for codec negotiation, as well as how many bytes will be present in each voice packet.

```
*Mar 12 04:03:57.217: cc_api_caps_ind (dstVdbPtr=0x616C9F54,
dstCallId=0x11, srcCallId=0x12, caps={codec=0xEBFB, fax_rate=0x7F,
vad=0x3, modem=0x617C5720 codec_bytes=0, signal_type=3})
*Mar 12 04:03:57.217: sess_appl: ev(23=CC_EV_CONF_CREATE_DONE),
cid(17), disp(0)
*Mar 12 04:03:57.217: ssa:
cid(17)st(3)oldst(0)cfid(7)csize(0)in(1)fDest(1)-cid2(18)st2(3)oldst2(
1)
*Mar 12 04:03:57.653: cc_api_caps_ind (dstVdbPtr=0x617BE064,
dstCallId=0x12, srcCallId=0x11, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
```

The following debug output shows that both parties negotiated correctly and agreed on G.711 codec with 160 bytes of data.

```
*Mar 12 04:03:57.653: cc_api_caps_ack (dstVdbPtr=0x617BE064,
dstCallId=0x12, srcCallId=0x11, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
*Mar 12 04:03:57.653: cc_api_caps_ind (dstVdbPtr=0x617BE064,
dstCallId=0x12, srcCallId=0x11, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x, codec_bytes=160, signal_type=0})
*Mar 12 04:03:57.653: cc_api_caps_ack (dstVdbPtr=0x617BE064,
dstCallId=0x12, srcCallId=0x11, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
*Mar 12 04:03:57.657: cc_api_caps_ack (dstVdbPtr=0x616C9F54,
dstCallId=0x11, srcCallId=0x12, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
*Mar 12 04:03:57.657: cc_api_caps_ack (dstVdbPtr=0x616C9F54,
dstCallId=0x11, srcCallId=0x12, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
```

The H.323 connect and disconnect messages follow.

```
*Mar 12 04:03:59.373: cc_api_call_connected(vdbPtr=0x617BE064,
callID=0x12)
*Mar 12 04:03:59.373: sess_appl: ev(8=CC_EV_CALL_CONNECTED), cid(18),
disp(0)
*Mar 12 04:03:59.373: ssa:
cid(18)st(4)oldst(1)cfid(7)csize(0)in(0)fDest(1)-cid2(17)st2(4)oldst2(
3)
*Mar 12 04:03:59.373: ccCallConnect (callID=0x11)
*Mar 12 04:03:59.373: {
*Mar 12 04:03:59.373:   h323-uu-pdu
*Mar 12 04:03:59.373:   {
*Mar 12 04:03:59.373:     h323-message-body connect :
```

```
*Mar 12 04:03:59.373:          {
*Mar 12 04:03:59.373:          protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:59.373:          h245Address ipAddress :
*Mar 12 04:03:59.373:          {
*Mar 12 04:03:59.377:              ip 'AC1046E2'H,
*Mar 12 04:03:59.377:              port 011008
*Mar 12 04:03:59.377:          },
*Mar 12 04:03:59.389: Hex representation of the CONNECT TPKT to
send.03000052080
*Mar 12 04:03:59.393: H225Lib::h225SetupResponse: Q.931 CONNECT sent
from socket [1]
*Mar 12 04:03:59.393: H225Lib::h225SetupResponse: Q.931 Call State
changed to [Active].
*Mar 12 04:04:08.769: cc_api_call_disconnected(vdbPtr=0x617BE064,
callID=0x12, cause=0x10)
*Mar 12 04:04:08.769: sess_appl: ev(12=CC_EV_CALL_DISCONNECTED),
cid(18), disp(0)
```

Cisco IOS Gateway with T1/PRI Interface

As explained earlier, two types of calls go through the Cisco IOS Gateways: the Cisco IOS Gateway interfaces to the PSTN or PBX with either T1/CAS or T1/PRI interfaces. The following example shows the debug outputs when the Cisco IOS Gateways use T1/PRI interface.

The debug isdn q931 command on the Cisco IOS Gateway has been turned on, enabling Q.931, a Layer Three signaling protocol for D-channel in the ISDN environment. Each time a call is placed out of the T1/PRI interface, a setup packet must be sent. The setup packet always has (protocol descriptor) pd = 8, and it generates a random hexadecimal value for the callref. The callref tracks the call. For example, if two calls are placed, the callref value can determine the call for which the RX (received) message is intended. Bearer capability 0x8890 means a 64 Kbps data call. If it were a 0x8890218F, it would be a 56 Kbps data call and 0x8090A3 if it is a voice call. In the debug output below, the bearer capability is 0x8090A3, which is for voice. The example shows called and calling party numbers.

The callref uses a different value for the first digit (to differentiate between TX and RX) and the second value is the same (SETUP had a 0 for the last digit and CONNECT_ACK also has a 0). The router completely depends upon the PSTN or PBX to assign a Bearer channel (B-channel). If the PSTN or PBX does not assign a channel to the router, the call will not be routed. In this case, a CONNECT

message is received from the switch with the same reference number as was received for ALERTING (0x800B). Finally, you can see the exchange of the DISCONNECT message followed by RELEASE and RELEASE_COMP messages as the call is being disconnected. A cause ID for the call rejection follows RELEASE_COMP messages. The cause ID is a hexadecimal value. The meaning of the cause can be found by decoding the hexadecimal value and following up with your provider.

```
*Mar 1 225209.694 ISDN Se115 TX -> SETUP pd = 8 callref = 0x000B
*Mar 1 225209.694 Bearer Capability i = 0x8090A3
*Mar 1 225209.694 Channel ID i = 0xA98381
*Mar 1 225209.694 Calling Party Number i = 0x2183, '1001'
*Mar 1 225209.694 Called Party Number i = 0x80, '3333'
*Mar 1 225209.982 ISDN Se115 RX <- ALERTING pd = 8 callref =
0x800B
*Mar 1 225209.982 Channel ID i = 0xA98381
*Mar 1 225210.674 ISDN Se115 RX <- CONNECT pd = 8 callref = 0x800B
*Mar 1 225210.678 ISDN Se115 TX -> CONNECT_ACK pd = 8 callref =
0x000B
*Mar 1 225215.058 ISDN Se115 RX <- DISCONNECT pd = 8 callref =
0x800B
*Mar 1 225215.058 Cause i = 0x8090 - Normal call clearing
225217 %ISDN-6
DISCONNECT Int S10 disconnected from unknown , call lasted 4 sec
*Mar 1 225215.058 ISDN Se115 TX -> RELEASE pd = 8 callref = 0x000B
*Mar 1 225215.082 ISDN Se115 RX <- RELEASE_COMP pd = 8 callref =
0x800B
*Mar 1 225215.082 Cause i = 0x829F - Normal, unspecified or Special
intercept, call blocked group restriction
```

Cisco IOS Gateway with T1/CAS Interface

Two types of calls go through the Cisco IOS Gateways: the Cisco IOS Gateway interface to the PSTN or PBX with either T1/CAS or T1/PRI interfaces. The following debug outputs occur when the Cisco IOS Gateways has T1/CAS interface. The debug cas on the Cisco IOS Gateway has been turned on.

The following debug message shows that the Cisco IOS Gateway is sending an off-hook signal to the switch.

```
Apr 5 17:58:21.727: from NEAT(0): (0/15): Tx LOOP_CLOSURE (ABCD=1111)
```

The following debug message indicates that the switch is sending wink after receiving the loop closure signal from the Cisco IOS Gateway.

```
Apr 5 17:58:21.859: from NEAT(0): (0/15): Rx LOOP_CLOSURE (ABCD=1111)
Apr 5 17:58:22.083: from NEAT(0): (0/15): Rx LOOP_OPEN (ABCD=0000)
```

The following debug message indicates that the Cisco IOS Gateway is going off-hook.

```
Apr 5 17:58:23.499: from NEAT(0): (0/15): Rx LOOP_CLOSURE (ABCD=1111)
```

The following output shows the show call active voice brief on the Cisco IOS Gateway when the call is in progress. The output also shows the called and calling party number and other useful information.

```
R5300-5#show call active voice brief
<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
tx:<packets>/<bytes> rx:<packets>/<bytes> <state>
  IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms
lost:<lost>/<early>/<late> delay:<last>/<min>/<max>ms <codec>
  FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
sig:<on/off> <codec> (payload size)
  Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l>
i/o:<l>/<l> dBm
511D : 156043737hs.1 +645 pid:0 Answer 1001 active
tx:1752/280320 rx:988/158080
  IP172.16.70.228:18888 rtt:0ms pl:15750/80ms lost:0/0/0
delay:25/25/65ms g711ulaw
511D : 156043738hs.1 +644 pid:1 Originate 3333 active
tx:988/136972 rx:1759/302548
  Tele 1/0/0 (30): tx:39090/35195/0ms g711ulaw noise:-43 acom:0
i/o:-36/-42 dBm
```




Case Study: Troubleshooting Intercluster Phone Calls

The case study in this appendix examines a Cisco IP Phone that is calling another Cisco IP Phone that is located in a different cluster. This type of call is also known as an intercluster Cisco IP Phone call.

This appendix contains the following topics:

- Sample Topology
- Intercluster H.323 Communication
- Call Flow Traces
- Failed Call Flow

Sample Topology

The following sample topology gets used in this case study. Two clusters, each having two Cisco CallManagers, and also Cisco IOS Gateways and a Cisco IOS Gatekeeper are in place.

Intercluster H.323 Communication

The Cisco IP Phone in Cluster 1 makes a call to the Cisco IP Phone in Cluster 2. Intercluster Cisco CallManager communication takes place using the H.323 Version 2 protocol. A Cisco IOS Gatekeeper also serves for admission control.

The Cisco IP Phone can connect to the Cisco CallManager via Skinny Station protocol, and the Cisco CallManager can connect with the Cisco IOS Gatekeeper by using the H.323 Registration, Admission, and Status (RAS) protocol. The admission request message (ARQ) gets sent to the Cisco IOS Gatekeeper, which sends the admission confirmed message (ACF) after making sure the intercluster call can be made using H.323 version 2 protocol. Once this happens, the audio path gets made by using the RTP protocol between Cisco IP Phones in different clusters.

Call Flow Traces

This section discusses the call flow by using SDI trace examples captured in the CCM000000000 file. The traces discussed in this case study focus only on the call flow itself.

In this call flow, a Cisco IP Phone (2002) located in Cluster 2 is calling a Cisco IP Phone (1001) located in Cluster 1. Remember that you can follow a device through the trace by looking at the TCP handle value, time stamp, or name of the device. The TCP handle value for the device remains the same until the device is rebooted or goes offline.

In the following traces, the Cisco IP Phone (2002) has gone off hook. The trace shows the unique messages, TCP handle, and the calling number, which displays on the Cisco IP Phone. The following debug output shows the called number (1001), H.225 connect, and H.245 confirm messages. The codec type is G.711 mu-law.

```
16:06:13.921 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x1c64310
16:06:13.953 CCM|Out Message -- H225ConnectMsg -- Protocol=
H225Protocol
16:06:13.953 CCM|Ie - H225UserUserIe IEData= 7E 00 37 05 02 C0 06
16:06:13.953 CCM|StationD - stationOutputCallInfo CallingPartyName=,
CallingParty=2002, CalledPartyName=1001, CalledParty=1001,
tcpHandle=0x1c64310
16:06:14.015 CCM|H245Interface(2) OLC indication chan number = 2
16:06:14.015 CCM|StationD - stationOutputOpenReceiveChannel
tcpHandle=0x1c64310 myIP: e74610ac (172.16.70.231)
16:06:14.015 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
16:06:14.062 CCM|StationInit - InboundStim -
StationOpenReceiveChannelAckID tcpHandle=0x1c64310, Status=0,
IpAddr=0xe74610ac, Port=20444, PartyID=2
```

```
16:06:14.062 CCM|H245Interface(2) paths established ip = e74610ac,
port = 20444
16:06:14.187 CCM|H245Interface(2) OLC outgoing confirm ip = fc4610ac,
port = 29626
```

The following traces show the calling and called party number, which associates with an IP address and a hexadecimal value.

```
16:06:14.187 CCM|StationD - stationOutputStartMediaTransmission
tcpHandle=0x1c64310 myIP: e74610ac (172.16.70.231)
16:06:14.187 CCM|StationD - RemoteIpAddr: fc4610ac (172.16.70.252)
```

The following traces show the packet sizes and the MAC address of the Cisco IP Phone (2002). The disconnect, then on-hook messages, follow these traces.

```
RemoteRtpPortNumber: 29626 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
16:06:16.515 CCM| Device SEP003094C26105 , UnRegisters with SDL Link
to monitor NodeID= 1
16:06:16.515 CCM|StationD - stationOutputCloseReceiveChannel
tcpHandle=0x1c64310 myIP: e74610ac (172.16.70.231)
16:06:16.515 CCM|StationD - stationOutputStopMediaTransmission
tcpHandle=0x1c64310 myIP: e74610ac (172.16.70.231)
16:06:16.531 CCM|In Message -- H225ReleaseCompleteMsg -- Protocol=
H225Protocol
16:06:16.531 CCM|Ie - Q931CauseIe -- IEData= 08 02 80 90
16:06:16.531 CCM|Ie - H225UserUserIe -- IEData= 7E 00 1D 05 05 80 06
16:06:16.531 CCM|Locations:Orig=1 BW=64Dest=0 BW=-1 (-1 implies
infinite bw available)
16:06:16.531 CCM|MediaManager - wait_AuDisconnectRequest - StopSession
sending disconnect to (64,2) and remove connection from list
16:06:16.531 CCM|MediaManager - wait_AuDisconnectReply - received all
disconnect replies, forwarding a reply for party1(16777219) and
party2(16777220)
16:06:16.531 CCM|MediaCoordinator - wait_AuDisconnectReply - removing
MediaManager(2) from connection list
16:06:16.734 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x1c64310
```

Failed Call Flow

The following section describes an unsuccessful intercluster call flow, as seen in the SDI trace. In the following traces, the Cisco IP Phone (1001) goes off hook. A TCP handle gets assigned to the Cisco IP Phone.

```
16:05:33.468 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x4fbbc30
16:05:33.468 CCM|StationD - stationOutputDisplayText
tcpHandle=0x4fbbc30, Display= 1001
16:05:33.484 CCM|StationD - stationOutputSetLamp stim: 9=Line
instance=1 lampMode=LampOn tcpHandle=0x4fbbc30
```

In the following traces, the user dials the called number (2000) of the Cisco IP Phone, and the process of digit analysis tries to match the number.

```
16:05:33.484 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="")
16:05:33.484 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
16:05:35.921 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="2")
16:05:35.921 CCM|Digit
analysis:potentialMatches=ExclusivelyOffnetPotentialMatchesExist
16:05:36.437 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="20")
16:05:36.437 CCM|Digit
analysis:potentialMatches=ExclusivelyOffnetPotentialMatchesExist
16:05:36.656 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="200")
16:05:36.656 CCM|Digit
analysis:potentialMatches=ExclusivelyOffnetPotentialMatchesExist
16:05:36.812 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="2000")
```

The digit analysis has now completed, and the results appear in the following traces. It is important to note that the following `PotentialMatches=NoPotentialMatchesExist` reference indicates that the Cisco CallManager cannot match this directory number. Finally, a reorder tone gets sent to the calling party (1001), which is followed by an on-hook message.

```
16:05:36.812 CCM|Digit analysis: analysis results
16:05:36.812 CCM||PretransformCallingPartyNumber=1001
|CallingPartyNumber=1001
|DialingPattern=2XXX
|DialingRoutePatternRegularExpression=(2XXX)
|PotentialMatches=NoPotentialMatchesExist
```

```
|CollectedDigits=2000
16:05:36.828 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001, CallingParty=1001, CalledPartyName=,
CalledParty=2000, tcpHandle=0x4fbbc30
16:05:36.828 CCM|StationD - stationOutputStartTone: 37=ReorderTone
tcpHandle=0x4fbbc30
16:05:37.953 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x4fbbc30
```

Failed Call Flow



A

access denied

troubleshooting **4-17**

add a new user does not work and you are
unable to access the administration

DC directory **5-11**

administration page not displaying

troubleshooting **4-4**

alarms

overview **2-6**

allowing remote access

how to **A-5**

application profiles do not display

troubleshooting **5-8**

AST

overview **2-5**

attachments

reports **A-4**

B

backup folder

troubleshooting **3-12**

backups

quick backup tips **3-2**

troubleshooting **3-9**

backup utility

unable to locate **3-12**

B-channel remains locked when restart_ack
does not contain channel IE

troubleshooting **6-29**

BIOS upgrade for MCS-7830

troubleshooting **3-6**

blank enterprise parameters page after upgrade

troubleshooting **3-8**

boot failure

recovery **3-4**

browser

unable to access administration page **4-6**

C

calls forwarded to voice mail treated as direct
call

troubleshooting **9-3**

cancelling backup process

troubleshooting **3-11**

CCO cases

opening a case **A-4**

- changing IIS parameters
 - troubleshooting **4-22**
- changing server name
 - troubleshooting **3-4**
- changing the IP address
 - troubleshooting **3-4**
- checking
 - RTP header compression **6-10**
- Cisco CallManager locks B-channel and sends restart
 - troubleshooting **6-25**
- Cisco CallManager service
 - overview **1-1**
- Cisco IP Phone
 - troubleshooting audio problems **6-5**
- Cisco Live!
 - reporting a case **A-5**
- Cisco Secure Telnet
 - design **A-6**
 - overview **2-18**
 - structure **A-6, A-7**
- Cisco Unity does not rollover
 - troubleshooting **9-3**
- CiscoWorks2000 **2-21**
- Code Red II
 - recovery **4-24**
- code red II recovery
 - virus protection **4-25**

- collecting
 - debugs **2-2**
 - sniffer traces **2-1**
- command line tools
 - overview **2-18**
- commands
 - show **2-18**
 - show command
 - options **2-19**
- compatibility matrix
 - hardware and software **1-3**
- control center
 - overview **2-13**
- counters
 - Microsoft performance **2-13**

D

- database corrupt after restore
 - troubleshooting **3-14**
- databases not in synch
 - troubleshooting **3-5**
- DC directory
 - add a new user does not work and you are unable to access the administration **5-11**
 - basic user search returns nothing **5-10**
 - troubleshooting **5-2**
 - users list not visible from Cisco CallManager Administration **5-10**

debugs

collecting 2-2

default web site under IIS has improper setting

troubleshooting 4-15

device issues

troubleshooting 6-1

diagnosing

slow server response 4-21

directory issues

troubleshooting 5-1

directory replication

troubleshooting 5-5

E

error code 1165

troubleshooting 3-11

F

features

troubleshooting 8-1, 9-1

G

guidelines

problem solving 1-3

H

hardware and software

compatibility matrix 1-3

I

installation

troubleshooting 3-3

IP Telephony networks

troubleshooting 1-5

L

LDAP replication

troubleshooting 5-7

logs

echo log 6-8

long term solutions

security 4-23

M

Microsoft Event Viewer

overview 2-17

Microsoft performance counters

overview 2-13

N

name to address resolution failing

troubleshooting **4-14**

near term solutions

security **4-23**

network failure

preparation **1-4**

no connectivity

remote server **4-18**

O

open a TAC case

required information **A-1**

opening a CCO case

url location **A-4**

overview **2-21**

alarms **2-6**

AST **2-5**

Cisco Secure Telnet **2-18**

CiscoWorks2000 **2-21**

command line tools **2-18**

control center **2-13**

Microsoft Event Viewer **2-17**

Microsoft performance counters **2-13**

of Cisco CallManager **1-1**

real-time monitoring **2-11**

serviceability **1-2, 2-5**

service activation **2-12**

show command **2-18**

traces **2-6**

troubleshooting **1-1**

P

port 80 blocked

troubleshooting **4-16**

preparation

network failure **1-4**

problem solving

guidelines **1-3**

Q

quick backup tips

troubleshooting **3-2**

R

real-time monitoring

overview **2-11**

recovery

boot failure **3-4**

Code Red II **4-24**

remote server

no connectivity **4-18**

unable to access administration page **4-14**

replication failure
 troubleshooting **4-20**

required information
 open a TAC case **A-1**

S

security
 long term solutions **4-23**
 near term solutions **4-23**
 troubleshooting **4-22**

security, firewall integrity **A-6**

serviceability
 overview **1-2**

serviceability tool
 overview **2-5**

service activation
 overview **2-12**

show
 commands **2-18**

show command
 options **2-19**
 overview **2-18**

sniffer traces
 collecting **2-1**

SNMP
 defined **2-20**
 remote monitoring with **2-20**

system
 troubleshooting **3-1**

system issues
 troubleshooting **4-1**

system not responding
 troubleshooting **4-2, 4-3**

T

TAC
 allowing remote access **A-5**
 Cisco Live! **A-5**
 required information **A-1**

TAC case
 attaching reports **A-4**

TAC web
 url location **A-4**

Telnet
 Cisco Secure Telnet **2-18**

Telnet, Cisco Secure
 design **A-6**
 structure **A-6, A-7**

testing
 Cisco CallManager configuration **6-10**
 gateways **6-8**

tips
 troubleshooting **2-22**

tools
 troubleshooting **2-1, 2-3**

- traces
 - overview 2-6
- troubleshooting
 - access denied 4-17
 - administration page not displaying 4-4
 - administrator account not associated with Cisco Unity subscriber 9-4
 - admission rejects 6-24
 - after restore database corrupt 3-14
 - application profiles do not display 5-8
 - ARJs 6-24
 - audio problems from Cisco IP Phone 6-5
 - backup error code 1165 3-11
 - backups 3-9
 - B-channel remains locked when restart_ack does not contain channel IE 6-29
 - BIOS for MCS-7830 3-6
 - blank enterprise parameters page 3-8
 - boot failure 3-4
 - browser server failed to retrieve backup list 3-7
 - calling search spaces 7-1
 - changing IIS parameters 4-22
 - changing server name 3-4
 - changing the IP address 3-4
 - Cisco CallManager locks B-channel and sends restart 6-25
 - Cisco CallManager system not responding 4-2
 - codec and region mismatches 6-11
 - Code Red II 4-24
 - conference bridge problems 8-1
 - databases not in synch 3-5
 - DC directory 5-2
 - default web site under IIS has improper setting 4-15
 - device issues 6-1
 - dial plan problems 7-4
 - directory issues 5-1
 - directory replication 5-5
 - dropped calls 6-13
 - echo 6-7
 - features 8-1, 9-1
 - gatekeeper issues 6-23
 - gateway registration failure 6-16
 - gateway reorder tone issues 6-15
 - H.225 gateway 6-24
 - installation 3-3
 - inter-cluster trunks 6-24
 - IP Telephony networks 1-5
 - LDAP replication 5-7
 - location and bandwidth issues 6-12
 - lost or distorted audio problems 6-2
 - MTP resource problems 8-6
 - name to address resolution failing 4-14
 - no connectivity to other devices 4-18
 - noise in recorded message 9-6
 - not authorized to view page 4-11
 - one-way or no audio 6-9
 - opening a case A-4
 - opening a case with TAC A-1

overview **1-1**
 phone resets **6-12**
 port 80 blocked **4-16**
 quick backup tips **3-2**
 registration rejects **6-25**
 remote access for TAC **A-5**
 replication failure **4-20**
 required preliminary information **A-1**
 route partition problems **7-1**
 RRJs **6-25**
 secure dial plans **7-6**
 security **4-22**
 sending attachments to TAC **A-4**
 system **3-1**
 system issues **4-1**
 system stops responding **4-3**
 TAC url location **A-4**
 tips **2-22**
 tools **2-3**
 transcoding problems **8-3**
 unable to access administration page from
 remote server **4-14**
 unable to access administration page from the
 browser **4-6**
 unable to cancel backup process **3-11**
 unable to locate backup folder **3-12**
 unable to locate backup utility **3-12**
 unity does not rollover **9-3**
 upgrades **3-6**
 using Cisco Live! **A-5**

viruses **4-9**
 voice mail stops after 30 seconds **9-1**
 voice messaging **9-1**
 voice quality issues **6-2**

U

unable to cancel backup process
 troubleshooting **3-11**
 upgrade
 blank enterprise parameters page **3-8**
 upgrades
 troubleshooting **3-6**
 URL location
 opening a CCO case **A-4**
 TAC web **A-4**

V

viruses
 troubleshooting **4-9**
 virus protection
 code red II recovery **4-25**
 voice mail stops after 30 seconds
 troubleshooting **9-1**
 voice messaging
 troubleshooting **9-1**

