Troubleshooting Guide for Cisco Unified Communications Manager, Release 12.5(1)

First Published: 2017-12-07

Last Modified: 2023-11-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xiii

Purpose xiii

Audience xiii

Organization xiv

Related Documentation xv

Conventions xv

Obtaining Documentation, Obtaining Support, and Security Guidelines xvi

Cisco Product Security Overview xvi

CHAPTER 1

Troubleshooting Overview 1

Cisco Unified Serviceability 1

Cisco Unified Communications Operating System Administration 2

General Model of Problem Solving 2

Network Failure Preparation 3

Where to Find More Information 3

CHAPTER 2

Troubleshooting Tools 5

Cisco Unified Serviceability Troubleshooting Tools 5

Command Line Interface 6

kerneldump Utility 7

Enable the Kerneldump Utility 8

Enable Email Alert for Core Dump 8

Network Management 9

System Log Management 9

Cisco Discovery Protocol Support 9

Simple Network Management Protocol Support 10

Sniffer Traces 10
Debugs 10
Cisco Secure Telnet 11
Packet Capture 11
Packet Capturing Overview 11
Configuration Checklist for Packet Capturing 12
Adding an End User to the Standard Packet Sniffer Access Control Group 13
Configuring Packet-Capturing Service Parameters 13
Configuring Packet Capturing in the Phone Configuration Window 14
Configuring Packet Capturing in Gateway and Trunk Configuration Windows 14
Packet-Capturing Configuration Settings 16
Analyzing Captured Packets 17
Common Troubleshooting Tasks, Tools, and Commands 17
Troubleshooting Tips 20
System History Log 21
System History Log Overview 21
System History Log Fields 22
Accessing the System History Log 23
Audit Logging 24
Verify Cisco Unified Communications Manager Services Are Running 28

CHAPTER 3 **Cisco Unified Communications Manager System Issues 31**
Cisco Unified Communications Manager System Not Responding 31
Cisco Unified Communications Manager System Stops Responding 32
Cisco Unified Communications Manager Administration Does Not Display 33
Error When Attempting to Access Cisco Unified Communications Manager Administration 33
Error When Attempting to Access Cisco Unified Communications Manager Administration on a Subsequent Node 33
You Are Not Authorized to View 34
Problems Displaying or Adding Users with Cisco Unified Communications Manager 34
Name to Address Resolution Failing 35
Port 80 Blocked Between Your Browser and the Cisco Unified Communications Manager Server 36
Improper Network Setting Exists in the Remote Machine 36
Manage Impact of Cisco RAID Operations 37

Database Replication 37
Replication Fails Between the Publisher and the Subscriber Server 38
Database Replication Does Not Occur When Connectivity Is Restored on Lost Node 41
Database Tables Out of Sync Do Not Trigger Alert 41
Resetting Database Replication When You Are Reverting to an Older Product Release 42
utils dbreplication clusterreset 43
utils dbreplication dropadmindb 43
LDAP Authentication Fails 43
Issues with LDAP Over SSL 44
Open LDAP Cannot Verify the Certificate to Connect to the LDAP Server 45
JTAPI Subsystem Startup Problems 46
JTAPI Subsystem is OUT_OF_SERVICE 46
MIVR-SS_TEL-4-ModuleRunTimeFailure 47
MIVR-SS_TEL-1-ModuleRunTimeFailure 49
JTAPI Subsystem is in PARTIAL_SERVICE 50
Security Issues 50
Security Alarms 51
Security Performance Monitor Counters 51
Reviewing Security Log and Trace Files 52
Troubleshooting Certificates 53
Troubleshooting Ciphers 53
Troubleshooting DRS and CDR Functionality 53
Troubleshooting CTL Security Tokens 54
Troubleshooting a Locked Security Token After You Consecutively Enter an Incorrect Security Token Password 54
Troubleshooting If You Lose One Security Token (Etoken) 54
Troubleshooting If You Lose All Security Tokens (Etoken) 55
Troubleshooting ITL Files 55
Troubleshooting CAPF 56
Troubleshooting the Authentication String on the Phone 56
Troubleshooting If the Locally Significant Certificate Validation Fails 56
Verifying That the CAPF Certificate Is Installed on All Servers in the Cluster 56
Verifying That a Locally Significant Certificate Exists on the Phone 57
Verifying That a Manufacture-Installed Certificate (MIC) Exists in the Phone 57

Troubleshooting Encryption for Phones and Cisco IOS MGCP Gateways 57
Using Packet Capturing 57
CAPF Error Codes 58

CHAPTER 4 **Device Issues 61**
Voice Quality 61
Lost or Distorted Audio 62
Correcting Audio Problems From the Cisco Unified IP Phone 63
Echo 64
One-Way Audio or No Audio 65
Codec and Region Mismatches 69
Location and Bandwidth 70
Phone Issues 70
Phone Resets 70
Dropped Calls 71
Phones Not Registering 72
Gateway Issues 72
Gateway Reorder Tone 72
Gateway Registration Failure 73
Gatekeeper Issues 78
Admission Rejects 78
Registration Rejects 79
B-Channel Remains Locked When Restart_Ack Does Not Contain Channel IE 79
Incorrect Device Registration Status Displays 80

CHAPTER 5 **Dial Plans and Routing Issues 81**
Route Partitions and Calling Search Spaces 81
Group Pickup Configuration 83
Dial Plan Issues 83
Problem When Dialing a Number 84
Secure Dial Plan 85
Automated Alternate Routing (AAR) Limitation with Remote Gateways 85

CHAPTER 6 **Cisco Unified Communications Manager Services Issues 87**

No Available Conference Bridge 87
Hardware Transcoder Not Working As Expected 89
No Supplementary Services Are Available on an Established Call 90

CHAPTER 7 Voice Messaging Issues 93
Voice Messaging Stops After 30 Seconds 93
Cisco Unity System Does Not Roll Over: Receive Busy Tone 94
Calls That Are Forwarded to Voice Messaging System Get Treated as a Direct Call to Cisco Unity System 94
Administrator Account Is Not Associated with Cisco Unity Subscriber 95

CHAPTER 8 Troubleshooting Features and Services 97
Troubleshooting Barge 97
Troubleshooting Call Back 98
Problems Using Call Back 98
User presses Callback softkey before phone rings 98
User unplugs or resets phone after pressing the CallBack softkey but before Call Back occurs 98
Caller misses availability notification before phone reset. Replace/retain screen does not explicitly state that availability notification occurred. 99
Error Messages for Call Back 100
Locating the Call Back Log Files 100
Troubleshooting Call Control Discovery 100
Troubleshooting Call Park 102
Troubleshooting Ciphers 103
Troubleshooting DRS and CDR Functionality 103
Troubleshooting Cisco Extension Mobility 103
Troubleshooting General Problems with Cisco Extension Mobility 104
Troubleshooting Cisco Extension Mobility Error Messages 104
Troubleshooting Cisco Unified Communications Manager Assistant 106
IPMAConsoleInstall.jsp Displays Error: HTTP Status 503-This Application is Not Currently Available 107
IPMAConsoleInstall.jsp Displays Error: No Page Found Error 107
Exception: java.lang.ClassNotFoundException: InstallerApplet.class 108
Automatic Installation of MS Virtual Machine Is No Longer Provided for Download 108

User Authentication Fails 109
Assistant Console Displays Error: System Error - Contact System Administrator 109
Assistant Console Displays Error: Cisco IP Manager Assistant Service Unreachable 110
Calls Do Not Get Routed When Filtering Is On or Off 111
Cisco IP Manager Assistant Service Cannot Initialize 112
Calling Party Gets a Reorder Tone 113
Manager Is Logged Out While the Service Is Still Running 113
Manager Cannot Intercept Calls That Are Ringing on the Assistant Proxy Line 114
Not Able to Call the Manager Phone When Cisco IP Manager Assistant Service is Down 114
Troubleshooting Cisco Unified Mobility 115
Cisco Unified Mobility User Hangs Up Mobile Phone But Cannot Resume Call on Desktop Phone 115
Dial-via-Office-Related SIP Error Codes 116
Troubleshooting Cisco Web Dialer 116
Authentication Error 117
Service Temporarily Unavailable 117
Directory Service Down 117
Cisco CTIManager Down 118
Session Expired, Please Login Again 118
User Not Logged in on Any Device 118
Failed to Open Device/Line 119
Destination Not Reachable 119
Troubleshooting Directed Call Park 119
Troubleshooting External Call Control 121
Troubleshooting Hotline 124
Troubleshooting Immediate Divert 125
Key Is Not Active 125
Temporary Failure 125
Busy 126
Troubleshooting Intercom 126
Getting Busy Tone When Dialing Out of Intercom Line 126
Intercom Calls Do Not Go to Connected State When Going Off Hook by Using Speaker, Handset, or Headset 126
Troubleshooting SCCP 127
Intercom Lines Not Showing Up on Phone When Button Template Has Them 127

Intercom Lines Not Showing Up When Phone Falls Back to SRST 127
Troubleshooting SIP 128
Debugging Phones That Are Running SIP 128
Configuration of Phones That Are Running SIP 128
Cisco Extension Mobility User Is Logged In But Intercom Line Does Not Display 128
Where to Find More Information 128
Troubleshooting IPv6 128
Phones Do Not Register with Cisco Unified Communications Manager 129
Calls Over SIP Trunks Fail 129
Calls Between Devices Fail 130
Music On Hold Does Not Play on Phone 130
Troubleshooting Logical Partitioning 130
Logical Partitioning Does Not Function As Expected 130
Logical Partitioning Policies Require Adjustment 131
Troubleshooting SIP with DNS Caching Enabled 133
Logging 133
Log file 133
Packet Capture 133
A/AAAA record caching is not working 134
Hostname resolution returning wrong IP address 135
Cannot find log 135
Set nscd attributes through CLI 135
CLI command to set TTL 136
A/AAAA Record Queries before TTL expires 136
Clearing the cache 136
Content of AAAA record cache 136
Troubleshooting SAML Single Sign On 137
Redirection to IdP fails 137
IdP Authentication Fails 137
Redirection to Unified Communications Manager fails 138
Run Test Fails 138
SAML Single Sign On Page Shows Incorrect Status on Cluster 138
General Tips 139

CHAPTER 9 SNMP Troubleshooting 141

Troubleshooting Tips 141

CISCO-CCM-MIB Tips 142

General Tips 142

Limitations 145

Frequently Asked Questions 146

HOST-RESOURCES-MIB Tips 151

Logs for Collection 151

Disk Space and RTMT 151

Frequently Asked Questions 152

CISCO-CDP-MIB Tips 154

General Tips 154

Frequently Asked Questions 154

SYSAPP-MIB Tips 154

Collecting Logs 155

Using Servlets in Cisco Unified Communications Manager 8.0 155

SNMP Developer Tips 156

Where to Find More Information 158

CHAPTER 10 Opening a Case With TAC 159

Information You Will Need 160

Required Preliminary Information 160

Network Layout 160

Problem Description 161

General Information 161

Online Cases 162

Serviceability Connector 162

Serviceability Connector Overview 162

Benefits of Using Serviceability Service 162

TAC Support for Serviceability Connector 163

Cisco Live! 163

Remote Access 163

Cisco Secure Telnet 164

Firewall Protection 164
Cisco Secure Telnet Design 164
Cisco Secure Telnet Structure 165
Set up a Remote Account 165

CHAPTER 11 Case Study: Troubleshooting Cisco Unified IP Phone Calls 167
Troubleshooting Intracluster Cisco Unified IP Phone Calls 167
Sample Topology 167
Cisco Unified IP Phone Initialization Process 168
Cisco Unified Communications Manager Initialization Process 169
Self-Starting Processes 169
Cisco Unified Communications Manager Registration Process 170
Cisco Unified Communications Manager KeepAlive Process 171
Cisco Unified Communications Manager Intracluster Call Flow Traces 171
Troubleshooting Intercluster Cisco Unified IP Phone Calls 175
Sample Topology 176
Intercluster H.323 Communication 176
Call Flow Traces 176
Failed Call Flow 177

CHAPTER 12 Case Study: Troubleshooting Cisco Unified IP Phone-to-Cisco IOS Gateway Calls 179
Call Flow Traces 179
Debug Messages and Show Commands on the Cisco IOS Gatekeeper 182
Debug Messages and Show Commands on the Cisco IOS Gateway 184
Cisco IOS Gateway with T1/PRI Interface 187
Cisco IOS Gateway with T1/CAS Interface 188

Preface

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

- Purpose, on page xiii
- Audience, on page xiii
- Organization, on page xiv
- Related Documentation, on page xv
- Conventions, on page xv
- Obtaining Documentation, Obtaining Support, and Security Guidelines, on page xvi
- Cisco Product Security Overview, on page xvi

Purpose

The *Troubleshooting Guide for Cisco Unified Communications Manager* provides troubleshooting procedures for this release of Unified Communications Manager.

Note The information in this version of the *Troubleshooting Guide for Unified Communications Manager* may not apply to earlier releases of the Unified Communications Manager software.

This document does not cover every possible trouble event that might occur on a Unified Communications Manager system but instead focuses on those events that are frequently seen by the Cisco Technical Assistance Center (TAC) or frequently asked questions from newsgroups.

Audience

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

Organization

The following table shows how this guide is organized.

Table 1: How This Document Is Organized

Chapter and Title	Description
Troubleshooting Overview, on page 1	Provides an overview of the tools and resources that are available for troubleshooting the Unified Communications Manager.
Troubleshooting Tools, on page 5	Addresses the tools and utilities that you can use to configure, monitor, and troubleshoot Unified Communications Manager and provides general guidelines for collecting information to avoid repetitive testing and re-collection of identical data.
Cisco Unified Communications Manager System Issues, on page 31	Describes solutions for the most common issues that relate to a Unified Communications Manager system.
Device Issues, on page 61	Describes solutions for the most common issues that relate to IP phones and gateways.
Dial Plans and Routing Issues, on page 81	Describes solutions for the most common issues that relate to dial plans, route partitions, and calling search spaces.
Cisco Unified Communications Manager Services Issues, on page 87	Describes solutions for the most common issues related to services, such as conference bridges and media termination points.
Voice Messaging Issues, on page 93	Describes solutions for the most common voice-messaging issues.
Troubleshooting Features and Services, on page 97	Provides information to help you resolve common issues with Unified Communications Manager features and services.
SNMP Troubleshooting, on page 141	Provides information on how to troubleshoot with SNMP
Opening a Case With TAC, on page 159	Describes what information is needed to open a case for TAC.
Case Study: Troubleshooting Cisco Unified IP Phone Calls, on page 167	Describes in detail the call flow between two Cisco Unified IP Phones within a cluster.
Case Study: Troubleshooting Cisco Unified IP Phone-to-Cisco IOS Gateway Calls, on page 179	Describes a Cisco Unified IP Phone calling through a Cisco IOS Gateway to a phone that is connected through a local PBX or on the Public Switched Telephone Network (PSTN).

Related Documentation

Refer to the *Cisco Unified Communications Manager Documentation Guide* for further information about related Cisco IP telephony applications and products. The following URL shows an example of the path to the documentation guide:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

For documentation that relates to Cisco Unity, refer to the following URL:

https://www.cisco.com/c/en/us/support/unified-communications/index.html

Conventions

This document uses the following conventions:

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

Notes use the following conventions:

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

Timesavers use the following conventions:

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

Tips use the following conventions:

Tip Means *the information contains useful tips*.

Cautions use the following conventions:

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

Warnings use the following conventions:

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

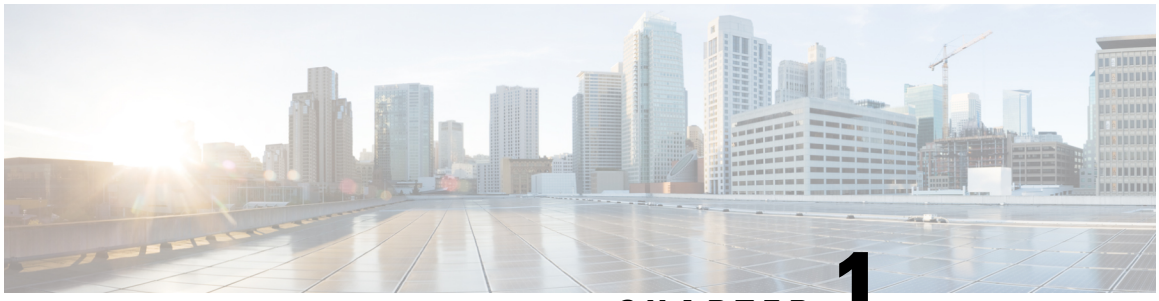
For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What''s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.



CHAPTER 1

Troubleshooting Overview

This section provides the necessary background information and available resources to troubleshoot the Unified Communications Manager.

- Cisco Unified Serviceability, on page 1
- Cisco Unified Communications Operating System Administration, on page 2
- General Model of Problem Solving, on page 2
- Network Failure Preparation, on page 3
- Where to Find More Information, on page 3

Cisco Unified Serviceability

Cisco Unified Serviceability, a web-based troubleshooting tool for Unified Communications Manager, provides the following functionality to assist administrators troubleshoot system problems:

- Saves Unified Communications Manager services alarms and events for troubleshooting and provides alarm message definitions.
- Saves Unified Communications Manager services trace information to various log files for troubleshooting. Administrators can configure, collect, and view trace information.
- Monitors real-time behavior of the components in a Unified Communications Manager cluster through the real-time monitoring tool (RTMT).
- Generates reports for Quality of Service, traffic, and billing information through Unified Communications Manager CDR Analysis and Reporting (CAR).
- Provides feature services that you can activate, deactivate, and view through the Service Activation window.
- Provides an interface for starting and stopping feature and network services.
- Archives reports that are associated with Cisco Unified Serviceability tools.
- Allows Unified Communications Manager to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a server (or all servers in the cluster).

Access Cisco Unified Serviceability from the Cisco Unified Communications Manager Administration window by choosing Cisco Unified Serviceability from the Navigation drop-down list box. Installing the Unified Communications Manager software automatically installs Cisco Unified Serviceability and makes it available.

See *Cisco Unified Serviceability Administration Guide* for detailed information and configuration procedures on the serviceability tools.

Cisco Unified Communications Operating System Administration

Cisco Unified Communications Operating System Administration allows you to perform the following tasks to configure and manage the *Cisco Unified Communications Operating System*:

- Check software and hardware status.
- Check and update IP addresses.
- Ping other network devices.
- Manage Network Time Protocol servers.
- Upgrade system software and options.
- Restart the system.

Refer to the Administration Guide for Cisco Unified Communications Manager for detailed information and configuration procedures on the serviceability tools.

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.

Procedure

1. Analyze the network problem and create a clear problem statement. Define symptoms and potential causes.
2. Gather the facts that you need to help isolate possible causes.
3. Consider possible causes based on the facts that you gathered.
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.
5. Implement the action plan; perform each step carefully while testing to see whether the symptom disappears.
6. Analyze the results to determine whether the problem has been resolved. If the problem was resolved, consider the process complete.
7. If the problem has not been resolved, create an action plan based on the next most probable cause on your list. Return to 4, on page 2 and repeat the process until the problem is 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 any filters configured in any of these bridges, and do you have a copy of these configurations? Is this applicable to Unified Communications Manager?
- 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.

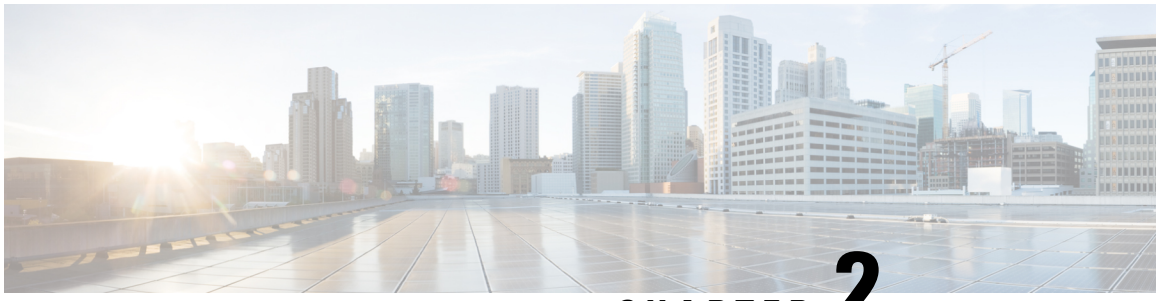
Where to Find More Information

Use the following links for information on various IP telephony topics:

- For further information about related Cisco IP telephony applications and products, see the *Cisco Unified Communications Manager Documentation Guide*. The following URL shows an example of the path to the documentation guide:

  https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html
- For documentation related to Cisco Unity, see the following URL:
  https://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html
- For documentation related to Cisco Emergency Responder, see the following URL:
  https://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

- For documentation related to Cisco Unified IP Phone, see the following URL: *https://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html*
- For information on designing and troubleshooting IP telephony networks, see the Cisco IP Telephony Solution Reference Network Design Guides that are available at: *https://www.cisco.com/go/srnd*



CHAPTER 2

Troubleshooting Tools

This section addresses the tools and utilities that you use to configure, monitor, and troubleshoot Unified Communications Manager and provides general guidelines for collecting information to avoid repetitive testing and recollection of identical data.

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

- Cisco Unified Serviceability Troubleshooting Tools, on page 5
- Command Line Interface, on page 6
- kerneldump Utility, on page 7
- Network Management, on page 9
- Sniffer Traces, on page 10
- Debugs, on page 10
- Cisco Secure Telnet, on page 11
- Packet Capture, on page 11
- Common Troubleshooting Tasks, Tools, and Commands, on page 17
- Troubleshooting Tips, on page 20
- System History Log, on page 21
- Audit Logging, on page 24
- Verify Cisco Unified Communications Manager Services Are Running, on page 28

Cisco Unified Serviceability Troubleshooting Tools

Refer to the *Cisco Unified Serviceability Administration Guide* for detailed information of the following different types of tools that Cisco Unified Serviceability provides to monitor and analyze the various Unified Communications Manager systems.

Table 2: Serviceability Tools

Term	Definition
Cisco Unified Real-Time Monitoring Tool (RTMT)	This tool provides real-time information about Unified Communications Manager devices and performance counters and enables you to collect traces. Performance counters can be system-specific or Unified Communications Manager specific. Objects comprise the logical groupings of like counters for a specific device or feature, such as Cisco Unified IP Phones or Unified Communications Manager System Performance. Counters measure various aspects of system performance. Counters measure statistics such as the number of registered phones, calls that are attempted and calls in progress.
Alarms	Administrators use alarms to obtain the run-time status and state of the Unified Communications Manager system. Alarms contain information about system problems such as explanation and recommended action. Administrators search the alarm definitions database for alarm information. The alarm definition contains a description of the alarm and recommended actions.
Trace	Administrators and Cisco engineers use trace files to obtain specific information about Unified Communications Manager service problems. Cisco Unified Serviceability sends configured trace information to the trace log file. Two types of trace log files exist: SDI and SDL. Every service includes a default trace log file. The system traces system diagnostic interface (SDI) information from the services and logs run-time events and traces to a log file. The SDL trace log file contains call-processing information from services such as Cisco CallManager and Cisco CTIManager. The system traces the signal distribution layer (SDL) of the call and logs state transitions into a log file. **Note** In most cases, you will only gather SDL traces when Cisco Technical Assistance Center (TAC) requests you to do so.
Quality Report Tool	This term designates voice quality and general problem-reporting utility in Cisco Unified Serviceability.
Serviceability Connector	The Cisco Webex Serviceability service increases the speed with which Cisco technical assistance staff can diagnose issues with your infrastructure. It automates the tasks of finding, retrieving, and storing diagnostic logs and information into an SR case. The service also triggers analysis against diagnostic signatures so that TAC can more efficiently identify and resolve issues with your on-premises equipment.

Command Line Interface

Use the command line interface (CLI) to access the Unified Communications Manager system for basic maintenance and failure recovery. Obtain access to the system by either a hard-wired terminal (a system monitor and keyboard) or by performing a SSH session.

The account name and password get created at install time. You can change the password after install, but you never can change the account name.

A command represents a text instruction that caused the system to perform some function. Commands may be stand alone, or they can have mandatory or optional arguments or options.

A level comprises a collection of commands; for example, show designates a level, whereas show status specifies a command. Each level and command also includes an associated privilege level. You can execute a command only if you have sufficient privilege level.

For complete information on the Unified Communications Manager CLI command set, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

kerneldump Utility

The kerneldump utility allows you to collect crash dump logs locally on the affected machine without requiring a secondary server.

In a Unified Communications Manager cluster, you only need to ensure the kerneldump utility is enabled on the server before you can collect the crash dump information.

Note Cisco recommends that you verify the kerneldump utility is enabled after you install Unified Communications Manager to allow for more efficient troubleshooting. If you have not already done so, enable the kerneldump utility before you upgrade the Unified Communications Manager from supported appliance releases.

Important Enabling or disabling the kerneldump utility will require a reboot of the node. Do not execute the enable command unless you are within a window where a reboot would be acceptable.

The *command line interface* (CLI) for the *Cisco Unified Communications Operating System* can be used to enable, disable, or check the status of the kerneldump utility.

Use the following procedure to enable the kernel dump utility:

Working with Files That Are Collected by the Utility

To view the crash information from the kerneldump utility, use the *Cisco Unified Real-Time Monitoring Tool* or the *Command Line Interface* (CLI). To collect the kerneldump logs by using the *Cisco Unified Real-Time Monitoring Tool*, choose the Collect Files option from Trace & Log Central. From the Select System Services/Applications tab, choose the Kerneldump logs check box. For more information on collecting files using *Cisco Unified Real-Time Monitoring Tool*, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

To use the CLI to collect the kerneldump logs, use the “file” CLI commands on the files in the crash directory. These are found under the “activelog” partition. The log filenames begin with the IP address of the kerneldump client and end with the date that the file is created. For more information on the file commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Enable the Kerneldump Utility

Use this procedure to enable the kerneldump utility. In the event of a kernel crash, the utility provides a mechanism for collecting and dumping the crash. You can configure the utility to dump logs to the local server or to an external server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Complete either of the following:

- To dump kernel crashes on the local server, run the `utils os kerneldump enable` CLI command.
- To dump kernel crashes to an external server, run the `utils os kerneldump ssh enable <ip_address>` CLI command with the IP address of the external server.

Step 3 Reboot the server.

Example

Note If you need to disable the kerneldump utility, you can run the `utils os kernelcrash disable` CLI command to disable the local server for core dumps and the `utils os kerneldump ssh disable <ip_address>` CLI command to disable the utility on the external server.

What to do next

Configure an email alert in the Real-Time Monitoring Tool to be advised of core dumps. For details, see Enable Email Alert for Core Dump, on page 8

Refer to the *Troubleshooting Guide for Cisco Unified Communications Manager* for more information on the kerneldump utility and troubleshooting.

Enable Email Alert for Core Dump

Use this procedure to configure the Real-Time Monitoring Tool to email the administrator whenever a core dump occurs.

Procedure

Step 1 Select **System** > **Tools** > **Alert** > **Alert Central**.

Step 2 Right-click **CoreDumpFileFound** alert and select **Set Alert Properties**.

Step 3 Follow the wizard prompts to set your preferred criteria:

a) In the **Alert Properties: Email Notification** popup, make sure that **Enable Email** is checked and click **Configure** to set the default alert action, which will be to email an administrator.
b) Follow the prompts and **Add** a Recipient email address. When this alert is triggered, the default action is to email this address.
c) Click **Save**.

Step 4 Set the default Email server:

a) Select **System** > **Tools** > **Alert** > **Config Email Server**.
b) Enter the e-mail server and port information to send email alerts.
c) Enter the **Send User Id**.
d) Click **OK**.

Network Management

Use the network management tools for Unified Communications Manager remote serviceability.

- System Log Management
- Cisco Discovery Protocol Support
- Simple Network Management Protocol support

Refer to the documentation at the URLs provided in the sections for these network management tools for more information.

System Log Management

Although it can be adapted to other network management systems, Cisco Syslog Analysis, which is packaged with Resource Manager Essentials (RME), provides the best method to manage Syslog messages from Cisco devices.

Cisco Syslog Analyzer serves as the component of Cisco Syslog Analysis that provides common storage and analysis of the system log for multiple applications. The other major component, Syslog Analyzer Collector, gathers log messages from Unified Communications Manager servers.

These two Cisco applications work together to provide a centralized system logging service for Cisco Unified Communications Solutions.

Refer to the following URL for RME documentation:
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

Cisco Discovery Protocol Support

The Cisco Discovery Protocol Support enables discovery of Unified Communications Manager servers and management of those servers.

Refer to the following URL for RME documentation:
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

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 Unified Communications Manager:
  - CiscoWorks Common Services Software
  - HP OpenView
  - Third-party applications that support SNMP and Unified Communications Manager SNMP interfaces

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 of 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, Unified Communications Managers, and so on.

Debugs

The output from **debug** privileged EXEC commands provides diagnostic information about a variety of internetworking event that relate 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 **`servicetimestampsdebugdatetimemsec`** 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 you must collect debugs in a live environment, configure **no logging console** and **loggingbuffered**. To collect the debugs, use **show log**.

Because some debugs can be lengthy, collect them directly on the console port (default **logging console**) or on the buffer (**logging buffer**). Collecting debugs over a Telnet session may impact the device performance, and the result could be incomplete debugs, which requires that you re-collect 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 Secure Telnet

Cisco Secure Telnet allows Cisco Service Engineers (CSE) transparent firewall access to the Unified Communications Manager 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 Unified Communications Manager 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.

Packet Capture

This section contains information about packet capture.

Related Topics

Packet Capturing Overview, on page 11
Configuration Checklist for Packet Capturing, on page 12
Adding an End User to the Standard Packet Sniffer Users..., on page 13
Configuring Packet-Capturing Service Parameters, on page 13
Configuring Packet Capturing in the Phone Configuration Window, on page 14
Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 14
Packet-Capturing Configuration Settings, on page 16
Analyzing Captured Packets, on page 17

Packet Capturing Overview

Because third-party troubleshooting tools that sniff media and TCP packets do not work after you enable encryption, you must use Unified Communications Manager to perform the following tasks if a problem occurs:

- Analyze packets for messages that are exchanged between Unified Communications Manager and the device [Cisco Unified IP Phone (SIP and SCCP), Cisco IOS MGCP gateway, H.323 gateway, H.323/H.245/H.225 trunk, or SIP trunk].
- Capture the Secure Real Time Protocol (SRTP) packets between the devices.
- Extract the media encryption key material from messages and decrypt the media between the devices.

Tip Performing this task for several devices at the same time may cause high CPU usage and call-processing interruptions. Cisco strongly recommends that you perform this task when you can minimize call-processing interruptions.

For more information, see the Security Guide for Cisco Unified Communications Manager.

Configuration Checklist for Packet Capturing

Extracting and analyzing pertinent data includes performing the following tasks.

Procedure

1. Add end users to the Standard Packet Sniffer Users group.
2. Configure packet capturing service parameters in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration; for example, configure the Packet Capture Enable service parameter.
3. Configure packet capturing settings on a per-device basis in the Phone or Gateway or Trunk Configuration window.

Note Cisco strongly recommends that you do not enable packet capturing for many devices at the same time because this task may cause high CPU usage in your network.

4. Capture SRTP packets by using a sniffer trace between the affected devices. Refer to the documentation that supports your sniffer trace tool.
5. After you capture the packets, set the Packet Capture Enable service parameter to False.
6. Gather the files that you need to analyze the packets.
7. Cisco Technical Assistance Center (TAC) analyzes the packets. Contact TAC directly to perform this task.

Related Topics

Adding an End User to the Standard Packet Sniffer Users..., on page 13
Analyzing Captured Packets, on page 17
Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 14
Configuring Packet Capturing in the Phone Configuration Window, on page 14
Configuring Packet-Capturing Service Parameters, on page 13
Packet-Capturing Configuration Settings, on page 16

Adding an End User to the Standard Packet Sniffer Access Control Group

End users that belong to the Standard Packet Sniffer Users group can configure the Packet Capture Mode and Packet Capture Duration settings for devices that support packet capturing. If the user does not exist in the Standard Packet Sniffer Access Control Group, the user cannot initiate packet capturing.

The following procedure, which describes how to add an end user to the Standard Packet Sniffer Access Control Group, assumes that you configured the end user in Cisco Unified Communications Manager Administration, as described in the Administration Guide for Cisco Unified Communications Manager.

Procedure

1. Find the access control group, as described in the Administration Guide for Cisco Unified Communications Manager.
2. After the Find/List window displays, click the **Standard Packet Sniffer Users** link.
3. Click the **Add Users to Group** button.
4. Add the end user, as described in the Administration Guide for Cisco Unified Communications Manager.
5. After you add the user, click **Save**.

Configuring Packet-Capturing Service Parameters

To configure parameters for packet capturing, perform the following procedure:

Procedure

1. In Unified Communications Manager, choose **System** > **Service Parameters**.
2. From the Server drop-down list box, choose an Active server where you activated the Cisco CallManager service.
3. From the Service drop-down list box, choose the **Cisco CallManager (Active)** service.
4. Scroll to the TLS Packet Capturing Configuration pane and configure the packet capturing settings.

Tip For information on the service parameters, click the name of the parameter or the question mark that displays in the window.

Note For packet capturing to occur, you must set the Packet Capture Enable service parameter to True.

5. For the changes to take effect, click **Save**.
6. You can continue to configure packet-capturing.

Related Topics

Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 14
Configuring Packet Capturing in the Phone Configuration Window, on page 14

Configuring Packet Capturing in the Phone Configuration Window

After you enable packet capturing in the Service Parameter window, you can configure packet capturing on a per-device basis in the Phone Configuration window of Cisco Unified Communications Manager Administration.

You enable or disable packet capturing on a per-phone basis. The default setting for packet capturing equals None.

Caution Cisco strongly recommends that you do not enable packet capturing for many phones at the same time because this task may cause high CPU usage in your network.

If you do not want to capture packets or if you completed the task, set the Packet Capture Enable service parameter to False.

To configure packet capturing for phones, perform the following procedure:

Procedure

1. Before you configure the packet-capturing settings, see the topics related to packet capturing configuration.
2. Find the SIP or SCCP phone, as described in the System Configuration Guide for Cisco Unified Communications Manager.
3. After the Phone Configuration window displays, configure the troubleshooting settings, as described in Packet-Capturing Configuration Settings.
4. After you complete the configuration, click **Save**.
5. In the Reset dialog box, click **OK**.

Tip Although Cisco Unified Communications Manager Administration prompts you to reset the device, you do not need to reset the device to capture packets.

Additional Steps

Capture SRTP packets by using a sniffer trace between the affected devices.

After you capture the packets, set the Packet Capture Enable service parameter to False.

Related Topics

Analyzing Captured Packets , on page 17
Configuration Checklist for Packet Capturing , on page 12

Configuring Packet Capturing in Gateway and Trunk Configuration Windows

The following gateways and trunks support packet capturing in Unified Communications Manager.

- Cisco IOS MGCP gateways
- H.323 gateways

- H.323/H.245/H.225 trunks
- SIP trunks

Tip Cisco strongly recommends that you do not enable packet capturing for many devices at the same time because this task may cause high CPU usage in your network.

If you do not want to capture packets or if you completed the task, set the Packet Capture Enable service parameter to False.

To configure packet-capturing settings in the Gateway or Trunk Configuration window, perform the following procedure:

Procedure

1. Before you configure the packet-capturing settings, see the topics related to packet capturing configuration.
2. Perform one of the following tasks:
   - Find the Cisco IOS MGCP gateway, as described in the System Configuration Guide for Cisco Unified Communications Manager.
   - Find the H.323 gateway, as described in the System Configuration Guide for Cisco Unified Communications Manager.
   - Find the H.323/H.245/H.225 trunk, as described in the System Configuration Guide for Cisco Unified Communications Manager.
   - Find the SIP trunk, as described in the System Configuration Guide for Cisco Unified Communications Manager.
3. After the configuration window displays, locate the Packet Capture Mode and Packet Capture Duration settings.

Tip If you located a Cisco IOS MGCP gateway, ensure that you configured the ports for the Cisco IOS MGCP gateway, as described in the Administration Guide for Cisco Unified Communications Manager. The packet-capturing settings for the Cisco IOS MGCP gateway display in the Gateway Configuration window for endpoint identifiers. To access this window, click the endpoint identifier for the voice interface card.

4. Configure the troubleshooting settings, as described in Packet-Capturing Configuration Settings.
5. After you configure the packet-capturing settings, click **Save**.
6. In the Reset dialog box, click **OK**.

Tip Although Cisco Unified Communications Manager Administration prompts you to reset the device, you do not need to reset the device to capture packets.

Additional Steps

Capture SRTP packets by using a sniffer trace between the affected devices.

After you capture the packets, set the Packet Capture Enable service parameter to False.

Related Topics

Analyzing Captured Packets , on page 17
Configuration Checklist for Packet Capturing , on page 12

Packet-Capturing Configuration Settings

The following table describes the Packet Capture Mode and Packet Capture Duration settings when configuring packet capturing for gateways, trunks, and phones.

Setting	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, Unified Communications Manager sets the Packet Capture Mode to None. • **Batch Processing Mode**— Unified Communications Manager writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Unified Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Unified Communications Manager stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. **Tip** Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.

Related Topics

Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 14
Configuring Packet Capturing in the Phone Configuration Window, on page 14

Analyzing Captured Packets

Cisco Technical Assistance Center (TAC) analyzes the packets by using a debugging tool. Before you contact TAC, capture SRTP packets by using a sniffer trace between the affected devices. Contact TAC directly after you gather the following information:

- Packet Capture File—**https://<IP address or server name>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**, where you browse into the server and locate the packet-capture file by month, date, and year (mm-dd-yyyy)
- Key for the file—**https://<IP address or server name>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**, where you browse into the server and locate the key by month, date, and year (mm-dd-yyyy)
- User name and password of end user that belongs to the Standard Packet Sniffer Users group

For more information, see Security Guide for Cisco Unified Communications Manager.

Common Troubleshooting Tasks, Tools, and Commands

This section provides a quick reference for commands and utilities to help you troubleshoot a Unified Communications Manager server with root access disabled. The following table provides a summary of the CLI commands and GUI selections that you can use to gather information troubleshoot various system problems.

Table 3: Summary of CLI Commands and GUI Selections

Information	Linux Command	Serviceability GUI Tool	CLI commands
CPU usage	top	RTMT Go to View tab and select **Server** > **CPU and Memory**	Processor CPU usage: show perf query class Processor Process CPU Usage for all processes: show perf query counter Process “% CPU Time” Individual process counter details (including CPU usage) show perf query instance <Process task_name>
Process state	ps	RTMT Go to View tab and select **Server** > **Process**	show perf query counter Process “Process Status”
Disk usage	df/du	RTMT Go to View tab and select **Server** > **Disk Usage**	show perf query counter Partition“% Used” or show perf query class Partition

Information	Linux Command	Serviceability GUI Tool	CLI commands
Memory	free	RTMT Go to View tab and select **Server** > **CPU and Memory**	show perf query class Memory
Network status	netstats		show network status
Reboot server	reboot	Log in to Platform Web page on the server Go to **Server** > **Current Version**	utils system restart
Collect Traces/logs	Sftp, ftp	RTMT Go to Tools tab and select **Trace** > **Trace & Log Central**	List file: file list Download files: file get View a file: file view

The following table provides a list of common problems and tools to use to troubleshoot them.

Table 4: Troubleshooting Common Problems with CLI Commands and GUI Selections

Task	GUI Tool	CLI commands
Accessing the database	none	Log in as admin and use any of the following **show** commands: • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* To run a SQL command, use the **run** command: • run sql <sql command>
Freeing up disk space **Note** You can only delete files from the Log partition.	Using the RTMT client application, go to the **Tools** tab and select **Trace & Log Central** > **Collect Files**. Choose the criteria to select the files you want to collect, then check the option **Delete Files**. This will delete the files on the Unified Communications Manager server after downloading the files to your PC.	file delete
Viewing core files	You cannot view the core files; however, you can download the Core files by using the RTMT application and selecting **Trace & Log Central** > **Collect Crash Dump**.	utils core [options.]

Task	GUI Tool	CLI commands
Rebooting the Unified Communications Manager server	Log in to Platform on the server and go to **Restart** > **Current Version**.	utils system restart
Changing debug levels for traces	Log in to *Cisco Unity Connection Serviceability* Administration at `https://<server_ipaddress>:8443/ccmservice/` and choose **Trace** > **Configuration**.	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
Looking at netstats	none	show network status

Troubleshooting Tips

The following tips may help you when you are troubleshooting the Unified Communications Manager.

Tip Check the release notes for Unified Communications Manager for known problems. The release notes provide descriptions and workaround solutions for known problems.

Tip Know where your devices are registered.

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

A common mistake involves having devices that are registered on a subscriber server but are capturing traces on the publisher server. These trace files will be nearly empty (and 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 Unified Communications Managers to obtain all the information that is needed to troubleshoot.

Tip Know the approximate time of the problem.

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

You can obtain phone statistics on a Cisco Unified IP Phone 79xx by pressing the **i** or**?** 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 the 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 time stamps in the file. The best way to collect the right trace means that you reproduce a problem and then quickly locate the most recent file and copy it from the Unified Communications Manager server.

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

Files will get 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.

System History Log

This system history log provides a central location for getting a quick overview of the initial system install, system upgrades, Cisco option installations, and DRS backups and DRS restores, as well as switch version and reboot history.

Related Topics

System History Log Overview, on page 21
System History Log Fields, on page 22
Accessing the System History Log, on page 23

System History Log Overview

The system history log exists as a simple ASCII file, **system-history.log**, and the data does not get maintained in the database. Because it does not get excessively large, the system history file does not get rotated.

The system history log provides the following functions:

- Logs the initial software installation on a server.
- Logs the success, failure, or cancellation of every software upgrade (Cisco option files and patches).
- Logs every DRS backup and restore that is performed.
- Logs every invocation of Switch Version that is issued through either the CLI or the GUI.
- Logs every invocation of Restart and Shutdown that is issued through either the CLI or the GUI.
- Logs every boot of the system. If not correlated with a restart or shutdown entry, the boot is the result of a manual reboot, power cycle, or kernel panic.

- Maintains a single file that contains the system history, since initial installation or since feature availability.
- Exists in the install folder. You can access the log from the CLI by using the **file** commands or from the Real Time Monitoring Tool (RTMT).

System History Log Fields

The log displays a common header that contains information about the product name, product version, and kernel image; for example:

==========

Product Name - Unified Communications Manager

Product Version - 7.1.0.39000-9023

Kernel Image - 2.6.9-67.EL

==========

Each system history log entry contains the following fields:

timestamp userid action description start/result

The system history log fields can contain the following values:

- *timestamp*—Displays the local time and date on the server with the format *mm/dd/yyyy hh:mm:ss*.
- *userid*—Displays the user name of the user who invokes the action.
- *action*—Displays one of the following actions:
  - Install
  - Windows Upgrade
  - Upgrade During Install
  - Upgrade
  - Cisco Option Install
  - Switch Version
  - System Restart
  - Shutdown
  - Boot
  - DRS Backup
  - DRS Restore
- *description*—Displays one of the following messages:
  - *Version*: Displays for the Basic Install, Windows Upgrade, Upgrade During Install, and Upgrade actions.
  - *Cisco Option file name*: Displays for the Cisco Option Install action.

- *Timestamp*: Displays for the DRS Backup and DRS Restore actions.
- *Active version to inactive version*: Displays for the Switch Version action.
- *Active version*: Displays for the System Restart, Shutdown, and Boot actions.

- *result*—Displays the following results:
  - Start
  - Success or Failure
  - Cancel

The following shows a sample of the system history log.

```
admin:file dump install system-history.log=======================================
Product Name -    Cisco Unified Communications Manager
Product Version - 6.1.2.9901-117
Kernel Image -    2.4.21-47.EL.cs.3BOOT
=======================================
07/25/2008 14:20:06 | root: Install 6.1.2.9901-117 Start
07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start
07/30/2008 10:08:56 | root: Upgrade 6.1.2.9901-126 Start
07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126 Success
07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Start

07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Success

07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start
08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126 Start
```

Accessing the System History Log

You can use either the CLI or RTMT to access the system history log.

Using the CLI

You can access the system history log by using the CLI **file** command; for example:

- **file view install system-history.log**
- **file get install system-history.log**

For more information on the CLI **file** commands, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Using RTMT

You can also access the system history log by using RTMT. From the Trace and Log Central tab, choose **Collect Install Logs**.

For more information about using RTMT, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Audit Logging

Centralized audit logging ensures that configuration changes to the Unified Communications Manager system gets logged in separate log files for auditing. An audit event represents any event that is required to be logged. The following Unified Communications Manager components generate audit events:

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability
- *Unified Communications Manager CDR Analysis and Reporting*
- *Cisco Unified Real-Time Monitoring Tool*
- *Cisco Unified Communications Operating System*
- *Disaster Recovery System*
- Database
- Command Line Interface
- Remote Support Account Enabled (CLI commands issued by technical supports teams)

In *Cisco Business Edition 5000*, the following Cisco Unity Connection components also generate audit events:

- Cisco Unity Connection Administration
- *Cisco Personal Communications Assistant* (Cisco PCA)
- Cisco Unity Connection Serviceability
- Cisco Unity Connection clients that use the Representational State Transfer (REST) APIs

The following example displays a sample audit event:

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:Successful
 Description: Call Manager Service status is stopped App ID:Cisco Tomcat Cluster
 ID:StandAloneCluster Node ID:sa-cm1-3
```

Audit logs, which contain information about audit events, get written in the common partition. The Log Partition Monitor (LPM) manages the purging of these audit logs as needed, similar to trace files. By default, the LPM purges the audit logs, but the audit user can change this setting from the Audit User Configuration window in Cisco Unified Serviceability. The LPM sends an alert whenever the common partition disk usage exceeds the threshold; however, the alert does not have the information about whether the disk is full because of audit logs or trace files.

Tip The Cisco Audit Event Service, which is a network service that supports audit logging, displays in Control Center—Network Services in Cisco Unified Serviceability. If audit logs do not get written, then stop and start this service by choosing **Tools** > **Control Center—Network Services** in Cisco Unified Serviceability.

All audit logs get collected, viewed and deleted from Trace and Log Central in the *Cisco Unified Real-Time Monitoring Tool*. Access the audit logs in RTMT in Trace and Log Central. Go to **System** > **Real-Time Trace** > **Audit Logs** > **Nodes**. After you select the node, another window displays **System** > **Cisco Audit Logs**.

The following types of audit logs display in RTMT:

- Application log
- Database log
- Operating system log
- Remote SupportAccEnabled log

Application Log

The application audit log, which displays in the AuditApp folder in RTMT, provides configuration changes for Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, the *CLI*, *Cisco Unified Real-Time Monitoring Tool* (RTMT), *Disaster Recovery System*, and Cisco Unified CDR Analysis and Reporting (CAR). For *Cisco Business Edition 5000*, the application audit log also logs changes for Cisco Unity Connection Administration, *Cisco Personal Communications Assistant* (Cisco PCA), Cisco Unity Connection Serviceability, and clients that use the Representational State Transfer (REST) APIs.

Although the Application Log stays enabled by default, you can configure it in Cisco Unified Serviceability by choosing **Tools** > **Audit Log Configuration**. For a description of the settings that you can configure for audit log configuration, see *Cisco Unified Serviceability Administration Guide*.

If the audit logs get disabled in Cisco Unified Serviceability, no new audit log files get created.

Tip Only a user with an audit role has permission to change the Audit Log settings. By default, the CCMAdministrator has the audit role after fresh installs and upgrades. The CCMAdministrator can assign the “standard audit users” group to a new user that the CCMAdministrator specifically creates for audit purposes. The CCMAdministrator can then be removed from the audit user group. The “standard audit log configuration” role provides the ability to delete audit logs, read/update access to *Cisco Unified Real-Time Monitoring Tool*, Trace Collection Tool, RTMT Alert Configuration, the Control Center - Network Services window, RTMT Profile Saving, the Audit Configuration window, and a new resource called Audit Traces. For Cisco Unity Connection in *Cisco Business Edition 5000*, the application administration account that was created during installation has the Audit Administrator role and can assign other administrative users to the role.

Unified Communications Manager creates one application audit log file until the configured maximum file size is reached; then, it closes and creates a new application audit log file. If the system specifies rotating the log files, Unified Communications Manager saves the configured number of files. Some of the logging events can be viewed by using RTMT SyslogViewer.

The following events get logged for Cisco Unified Communications Manager Administration:

- User logging (user logins and user logouts).
- User role membership updates (user added, user deleted, user role updated).
- Role updates (new roles added, deleted, or updated).
- Device updates (phones and gateways).
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, host names, Ethernet settings, and Unified Communications Manager server additions or deletions).

The following events get logged for Cisco Unified Serviceability:

- Activation, deactivation, start, or stop of a service from any Serviceability window.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.
- Changes in CDR Management.
- Review of any report in the Serviceability Reports Archive. View this log on the reporter node.

RTMT logs the following events with an audit event alarm:

- Alert configuration.
- Alert suspension.
- E-mail configuration.
- Set node alert status.
- Alert addition.
- Add alert action.
- Clear alert.
- Enable alert.
- Remove alert action.
- Remove alert.

The following events get logged for *Unified Communications Manager CDR Analysis and Reporting*:

- Scheduling the CDR Loader.
- Scheduling the daily, weekly, and monthly user reports, system reports, and device reports.
- Mail parameters configurations.
- Dial plan configurations.
- Gateway configurations.
- System preferences configurations.
- Autopurge configurations.

- Rating engine configurations for duration, time of day, and voice quality.
- QoS configurations.
- Automatic generation/alert of pregenerated reports configurations.
- Notification limits configurations.

The following events gets logged for *Disaster Recovery System*:

- Backup initiated successfully/failed
- Restore initiated successfully/failed
- Backup cancelled successfully
- Backup completed successfully/failed
- Restore completed successfully/failed
- Save/update/delete/enable/disable of backup schedule
- Save/update/delete of destination device for backup

For *Cisco Business Edition 5000*, Cisco Unity Connection Administration logs the following events:

- User logging (user logins and user logouts).
- All configuration changes, including but not limited to users, contacts, call management objects, networking, system settings, and telephony.
- Task management (enabling or disabling a task).
- Bulk Administration Tool (bulk creates, bulk deletes).
- Custom Keypad Map (map updates)

For *Cisco Business Edition 5000*, Cisco PCA logs the following events:

- User logging (user logins and user logouts).
- All configuration changes made via the Messaging Assistant.

For *Cisco Business Edition 5000*, Cisco Unity Connection Serviceability logs the following events:

- User logging (user logins and user logouts).
- All configuration changes.
- Activating, deactivating, starting or stopping services.

For *Cisco Business Edition 5000*, clients that use the REST APIs log the following events:

- User logging (user API authentication).
- API calls that utilize Cisco Unity Connection Provisioning Interface (CUPI).

Database Log

The database audit log, which displays in the informix folder in RTMT, reports database changes. This log, which is not enabled by default, gets configured in Cisco Unified Serviceability by choosing **Tools** > **Audit Log Configuration**. For a description of the settings that you can configure for audit log configuration, see Cisco Unified Serviceability.

This audit differs from the Application audit because it logs database changes, and the Application audit logs application configuration changes. The informix folder does not display in RTMT unless database auditing is enabled in Cisco Unified Serviceability.

Operating System Log

The operating system audit log, which displays in the vos folder in RTMT, reports events that are triggered by the operating system. It does not get enabled by default. The **utils auditd** CLI command enables, disables, or gives status about the events.

The vos folder does not display in RTMT unless the audit is enabled in the CLI.

For information on the CLI, see *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Remote Support Acct Enabled Log

The Remote Support Acct Enabled audit log, which displays in the vos folder in RTMT, reports CLI commands that get issued by technical support teams. You cannot configure it, and the log gets created only if the Remote Support Acct gets enabled by the technical support team.

Verify Cisco Unified Communications Manager Services Are Running

Use the following procedure to verify which Cisco CallManager services are active on a server.

Procedure

1. From Cisco Unified Communications Manager Administration, choose **Navigation** > **Cisco Unified Serviceability**.
2. Choose **Tools** > **Service Activation**.
3. From the Servers column, choose the desired server.

   The server that you choose displays next to the Current Server title, and a series of boxes with configured services displays.

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

   If the **Activated** status displays, the specified Cisco CallManager service remains active on the chosen server.

   If the **Deactivated** status displays, continue with the following steps.
4. Check the check box for the desired Cisco CallManager service.
5. Click the **Update** button.

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

The specified service now shows active for the chosen server.

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

Procedure

1. From Cisco Unified Communications Manager Administration, choose **Navigation** > **Cisco Unified Serviceability**.

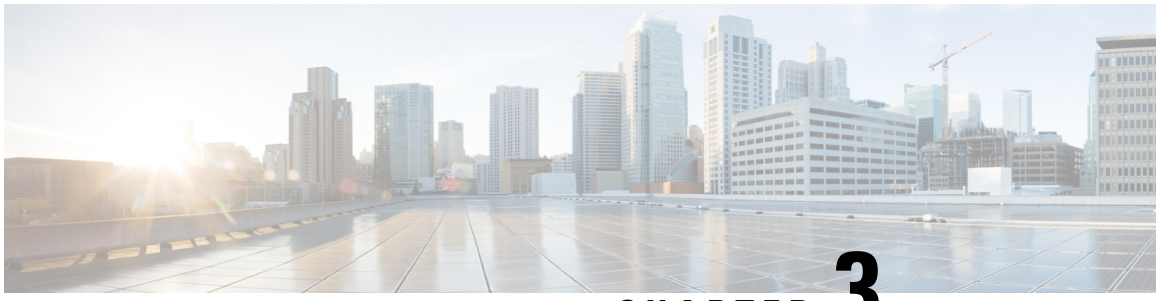
   The Cisco Unified Serviceability window displays.

2. Choose **Tools** > **Control Center – Feature Services**.

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 Status column displays which services are running for the chosen server.



CHAPTER 3

Cisco Unified Communications Manager System Issues

This section covers solutions for the most common issues that relate to a Unified Communications Manager system.

- Cisco Unified Communications Manager System Not Responding, on page 31
- Database Replication, on page 37
- LDAP Authentication Fails, on page 43
- Issues with LDAP Over SSL, on page 44
- Open LDAP Cannot Verify the Certificate to Connect to the LDAP Server, on page 45
- JTAPI Subsystem Startup Problems, on page 46
- Security Issues, on page 50

Cisco Unified Communications Manager System Not Responding

This section covers issues related to a Unified Communications Manager system that is not responding.

Related Topics

Cisco Unified Communications Manager System Stops Responding, on page 32
Cisco Unified Communications Manager Administration Does Not Display, on page 33
Error When Attempting to Access Cisco Unified Communications Manager Administration..., on page 33
Error When Attempting to Access Cisco Unified Communications Manager Administration..., on page 33
You Are Not Authorized to View, on page 34
Problems Displaying or Adding Users with Cisco Unified Communications Manager..., on page 34
Name to Address Resolution Failing, on page 35
Port 80 Blocked Between Your Browser and the Cisco Unified..., on page 36
Improper Network Setting Exists in the Remote Machine, on page 36
Slow Server Response

Cisco Unified Communications Manager System Stops Responding

Symptom

The Unified Communications Managersystem does not respond.

When the Cisco CallManager service stops responding, the following message displays in the System Event log:

```
The Cisco CallManager service terminated unexpectedly. It has done this 1 time.
The following corrective action
will be taken in 60000 ms. Restart the service.
```

Other messages you may see in this situation:

```
Timeout 3000 milliseconds waiting for Cisco CallManager service to connect.
```

The Cisco Communications Manager failed to start due to the following error:

```
The service did not respond to the start or control request in a timely fashion.
```

At this time, when devices such as the Cisco Unified IP Phones and gateways unregister from the Unified Communications Manager, users receive delayed dial tone, and/or the Unified Communications Managerserver freezes due to high CPU usage. For event log messages that are not included here, view the Unified Communications Manager Event Logs.

Possible Cause

The Cisco CallManager service can stop responding because the service does not have enough resources such as CPU or memory to function. Generally, the CPU utilization in the server is 100 percent at that time.

Recommended Action

Depending on what type of interruption you experience, you will need to gather different data that will help determine the root cause of the interruption.

Use the following procedure if a lack of resources interruption occurs.

Procedure

1. Collect Cisco CallManager traces 15 minutes before and after the interruption.
2. Collect SDL traces 15 minutes before and after the interruption.
3. Collect perfmon traces if available.
4. If the traces are not available, start collecting the perfmon traces and track memory and CPU usage for each process that is running on the server. These will help in the event of another lack of resources interruption.

Cisco Unified Communications Manager Administration Does Not Display

Symptom

Cisco Unified Communications Manager Administration does not display.

Possible Cause

The Cisco CallManager service stopped.

Recommended Action

Verify that the Cisco CallManager service is active and running on the server. See related topics or the *Cisco Unified Serviceability Administration Guide*.

Related Topics

Verify Cisco Unified Communications Manager Services Are Running, on page 28

Error When Attempting to Access Cisco Unified Communications Manager Administration

Symptom

An error message displays when you are trying to access Unified Communications Manager.

Possible Cause

The services did not start automatically as expected. One of the services stopping represents the most frequent reason for Cisco Unified Communications Manager Administration not displaying.

Recommended Action

Try starting the other services.

Error When Attempting to Access Cisco Unified Communications Manager Administration on a Subsequent Node

Symptom

An error message displays when you are trying to access the Unified Communications Manager Administration.

Possible Cause

If the IP address of the first Unified Communications Manager node gets changed while a subsequent node is offline, you may not be able to log in to Cisco Unified Communications Manager Administration on the subsequent node.

Recommended Action

If this occurs, follow the procedure for changing the IP address on a subsequent Unified Communications Manager node in the document, *Changing the IP Address and Host Name for Unified Communications Manager*.

You Are Not Authorized to View

Symptom

When you access Unified Communications Manager Administration, one of the following messages displays.

- You Are Not Authorized to View This Page
- You do not have permission to view this directory or page using the credentials you supplied.
- 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.

Possible Cause

Unknown

Recommended Action

Contact TAC for further assistance.

Problems Displaying or Adding Users with Cisco Unified Communications Manager

Symptom

You cannot add a user or conduct a search in Unified Communications Manager.

Possible Cause

You may encounter the following problems if you are working with Unified Communications Manager that is installed on a server that has a special character (such as an underscore) in its hostname or Microsoft Internet Explorer 5.5 with SP2 and a Q313675 patch or above.

- When you conduct a basic search and click submit, the same page redisplays.
- When you try to insert a new user, the following message displays.

```
The following error occurred while trying to execute the command.Sorry, your
 session object has timed out.
Click here to Begin a New Search
```

Recommended Action

You may not be able to add a user or do a search on Unified Communications Manager Administration, if your Unified Communications Manager hostname contains any special characters such as underscore or period (for example, Call_Manager). Domain Name System (DNS)-supported characters include all letters (A-Z, a-z), numbers (0-9), and hyphen (-); any special characters are not allowed. If the Q313675 patch is installed on your browser, make sure that the URL does not contain any non-DNS supported characters.

For more information about the Q313675 patch, refer to MS01-058: File Vulnerability Patch for Internet Explorer 5.5 and Internet Explorer 6.

To resolve this problem, you have the following options:

- Access Cisco Unified Communications Manager Administration by using the IP address of the server.
- Do not use non-DNS characters in the Server Name.
- Use the localhost or IP address in the URL.

Name to Address Resolution Failing

Symptom

One of the following 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 by using the Cisco Communications Manager IP address (`http://10.48.23.2/ccmadmin`) instead of the name, the window displays.

Possible Cause

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

Recommended Action

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 Unified Communications Manager server. If it is not correct, change it.

If you are not using DNS, your local machine will check in the "hosts" file to see whether an entry exists for the *your-cm-server-name* and an IP address that is associated to it. Open the file and add the Unified Communications Manager server name and the IP address. You can find the "hosts" file at `C:\WINNT\system32\drivers\etc\hosts`.

Port 80 Blocked Between Your Browser and the Cisco Unified Communications Manager Server

Symptom

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

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

Possible Cause

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

Recommended Action

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

Improper Network Setting Exists in the Remote Machine

Symptom

No connectivity exists, or no connectivity exists to other devices in the same network as the Unified Communications Manager.

When you attempt the same action from other remote machines, Unified Communications Manager Administration displays.

Possible 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.

Recommended Action

1. Try pinging the IP address of the Unified Communications Manager server and other devices to confirm that you cannot connect.
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. 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.

3. Choose **Start** > **Setting** > **Network and Dial-up connections**.
4. Choose **Local Area Connection**, then **Properties**.

   The list of communication protocols displays as checked.
5. Choose **Internet Protocol (TCP-IP)** and click **Properties** again.
6. 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.
7. Choose the Internet Explorer browser **Tools** > **Internet Options**.
8. 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 do not get configured. The generic network setting from Windows gets used.
9. If the connectivity is failing only to the Unified Communications Manager 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.

Manage Impact of Cisco RAID Operations

Cisco Redundant Array of Independent Disks (RAID) Controller conducts background operations such as Consistency Check (CC), Background Initialization (BGI), Rebuild (RBLD), Volume Expansion & Reconstruction (RLM) and Patrol Real (PR).

These background operations are expected to limit their impact to I/O operations. However, there have been cases of higher impact during some of the operations like Format or similar input output operations. In these cases, both the I/O operation and the background operations may consume large amount of CPU resources. It is recommended that CC and Patrol Read jobs are scheduled when the load is relatively less. If there are CallManager servers where huge load is running at the same time, it is recommend that you limit possible concurrent background operations and other intensive I/O operations of CallManager.

Database Replication

This section covers database replication issues for aUnified Communications Manager system.

Related Topics

Replication Fails Between the Publisher and the Subscriber Server, on page 38
Database Replication Does Not Occur When Connectivity Is Restored on..., on page 41
Database Tables Out of Sync Do Not Trigger Alert, on page 41
Resetting Database Replication When You Are Reverting to an Older..., on page 42

Replication Fails Between the Publisher and the Subscriber Server

Replicating the database represents a core function of Unified Communications Manager clusters. The server with the master copy of the database acts as the publisher (first node), while the servers that replicate the database comprise subscribers (subsequent nodes).

Tip Before you install Unified Communications Manager on the subscriber server, you must add the subscriber to the Server Configuration window in Cisco Unified Communications Manager Administration to ensure that the subscriber replicates the database that exists on the publisher database server. After you add the subscriber server to the Server Configuration window and then install Unified Communications Manager on the subscriber, the subscriber receives a copy of the database that exists on the publisher server.

Symptom

Changes that are made on the publisher server do not get reflected on phones that are registered with the subscriber server.

Possible Cause

Replication fails between the publisher and subscriber servers.

Recommended Action

Verify and, if necessary, repair database replication, as described in the following procedure:

Procedure

1. Verify database replication. You can use the CLI, Cisco Unified Reporting , or RTMT to verify database replication.
   - To verify by using the CLI, see 2, on page 38 .
   - To verify by using Cisco Unified Reporting, see 3, on page 39 .
   - To verify by using RTMT, see 4, on page 39 .
2. To verify database replication by using the CLI, access the CLI and issue the following command to check replication on each node. You will need to run this CLI command on each node to check its replication status. Also, after a subscriber is installed, depending on the number of subscribers, it may take a considerable amount of time to archive a status of 2.

```
admin:

              show perf query class "Number of Replicates Created and State of
Replication"


            ==>query class: - Perf class (Number of Replicates Created and
State of Replication) has instances and values: ReplicateCount -> Number of
Replicates Created = 344 ReplicateCount -> Replicate_State = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0—This value indicates that replication did not start. Either no subsequent nodes (subscribers) exist, or the Cisco Database Layer Monitor service is not running and has not been running since the subscriber was installed.
- 1—This value indicates that replicates have been created, but their count is incorrect.
- 2—This value indicates that replication is good.
- 3—This value indicates that replication is bad in the cluster.
- 4—This value indicates that replication setup did not succeed.

3. To verify database replication by using Cisco Unified Reporting, perform the following tasks.
   a. From the Navigation drop-down list box in the upper, right corner in Cisco Unified Communications Manager Administration, choose **Cisco Unified Reporting** .
   b. After Cisco Unified Reporting displays, click **System Reports** .
   c. Generate and view the **Unified CM Database Status** report, which provides debugging information for database replication.

      Once you have generated the report, open it and look at the **Unified CM Database Status** . It gives the RTMT replication counters for all servers in the cluster. All servers should have a replicate state of 2, and all servers should have the same number of replicates created.

      If you see any servers whose replicate states are not equal to 2 in the above status check, inspect the "Replication Server List" on this report. It shows which servers are connected and communicating with each node. Each server should show itself as local (in its list) and the other servers as active connected. If you see any servers as dropped, it usually means there is a communication problem between the nodes.
   d. If you want to do so, generate and view the **Unified CM Database Status** report, which provides a snapshot of the health of the Unified Communications Manager database.

4. To verify database replication by using RTMT, perform the following tasks:
   a. Open the Cisco Unified Real-Time Monitoring Tool (RTMT).
   b. Click the **CallManager** tab.
   c. Click **Database Summary** . The Replication Status pane displays.

   The following list shows the possible values for the Replication Status pane:

   - 0—This value indicates that replication has not started. Either no subsequent nodes (subscribers) exist, or the Cisco Database Layer Monitor service is not running and has not been running since the subscriber was installed.
   - 1—This value indicates that replicates have been created, but their count is incorrect.
   - 2—This value indicates that replication is good.
   - 3—This value indicates that replication is bad in the cluster.
   - 4—This value indicates that replication setup did not succeed.
   - To view the Replicate_State performance monitoring counter, choose **System** > **Performance** > **Open Performance Monitoring** . Double-click the publisher database server (first node) to expand

the performance monitors. Click **Number of Replicates Created and State of Replication** . Double-click **Replicate_State** . Click **ReplicateCount** from the Object Instances window and click **Add** .

Tip To view the definition of the counter, right click the counter name and choose **Counter Description** .

5. If all the servers have a good RTMT status, but you suspect the databases are not in sync, you can run the CLI command **utils dbreplication status**

   (If any of the servers showed an RTMT status of 4, proceed to Step 6)

   This status command can be run on all servers by using **utils dbreplication status all**

   or on one subscriber by using **utils dbreplication status** <*hostname*>

   The status report will tell you if any tables are suspect. If there are suspect tables, you will want to do a replication repair CLI command to sync the data from the publisher server to the subscriber servers.

   The replication repair can be done on all subscriber servers (using the **all** parameter) or on just one subscriber server by using the following:

   utils dbreplication repair usage:utils dbreplication repair [nodename]|all

   After running the replication repair, which can take several minutes, you can run another status command to verify that all tables are now in sync.

   If tables are in sync after running the repair, you are successful in fixing replication.

Note Only do Step 6 if one of the servers showed an RTMT status of 4, or had a status of 0 for more than four hours.

6. Generate and view the **Unified CM Database Status** report, which provides debugging information for database replication. For each subscriber server that has a bad RTMT status, check that the hosts, rhosts, sqlhosts, and services files have the appropriate information.

   Generate and view the **Unified CM Cluster Overview** report. Verify that the subscriber servers have the same version, verify that connectivity is good, and verify that time delay is within tolerances.

   If the preceding conditions are acceptable, do the following to reset replication on that subscriber server:

   a. At the subscriber server, perform the CLI command **utils dbreplication stop**

      Do this for all subscriber servers that have an RTMT value of 4

   b. At the publisher server, perform the CLI command **utils dbreplication stop**

   c. At the publisher server, perform the CLI command **utils dbreplication reset** <*hostname*>

      where <*hostname*> is the hostname of the subscriber server that needs to be reset. If all subscriber servers need to be reset, use command **utils dbreplication reset all**

For More Information

Cisco Unified Real-Time Monitoring Tool Administration Guide

Cisco Unified Reporting Administration Guide

Command Line Interface Reference Guide for Cisco Unified Solutions

Database Replication Does Not Occur When Connectivity Is Restored on Lost Node

Symptom

Database replication does not occur when connectivity is restored on lost node recovery. See the related topics for methods to verify the state of replication if replication fails. Only use the following procedure if you have already tried to reset replication on the node, and have been unsuccessful.

Possible Cause

The CDR check remains stuck in a loop, due to a delete on device table.

Recommended Action

1. Run **utils dbreplication stop** on the affected subscribers. You can run them all at once.
2. Wait until step 1 completes, then run **utils dbreplication stop** on the affected publisher server.
3. Run **utils dbreplication clusterreset** from the affected publisher server. When you run the command, the log name gets listed in the log file. Watch this file to monitor the process status. The path to the follows:

   `/var/log/active/cm/trace/dbl/sdi`
4. From the affected publisher, run **utils dbreplication reset all**.
5. Stop and restart all the services on all the subscriber servers [or restart/reboot all the systems (subscriber servers)] in the cluster to get the service changes. Do this only after **utils dbreplication status** shows Status 2.

Related Topics

Replication Fails Between the Publisher and the Subscriber Server, on page 38

Database Tables Out of Sync Do Not Trigger Alert

Note "Out of sync" means that two servers in the cluster do not contain the same information in a specific database table.

Symptom

On Unified Communications Manager Version 6.x or later, the symptoms include unexpected call processing behaviors. Calls do not get routed or handled as expected. The symptoms may occur on either the publisher or on the subscriber servers.

On Unified Communications Manager Version 5.x, the symptoms include unexpected call processing behaviors. Calls do not get routed or handled as expected but only when the publisher server is offline.

If you see this symptom and you run **utils dbrepication status** at the CLI, it reports `Out of sync`.

If `Out of sync` does not display, be aware that this is not the problem.

Possible Cause

Database tables remain out of sync between nodes. Replication alerts only indicate failure in the replication process and do not indicate when database tables are out of sync. Normally, if replication is working, tables should remain in sync. Instances can occur in which replication appears to be working, but database tables are “Out of sync”.

Recommended Action

1. Reset cluster replication by using CLI commands. Ensure servers in the cluster are online with full IP connectivity for this to work. Confirm that all servers in the cluster are online by using platform CLIs and *Cisco Unified Reporting*.
2. If the servers are in Replication State 2, run the following command on the publisher server:
3. **utils dbreplication repair** *server name*
4. If the servers are not in Replication State 2,
5. run the following command on all subscriber servers:
6. **utils dbreplication stop**
7. Then, run the following commands on the publisher server:
8. **utils dbreplication stop**
9. then
10. **utils dbreplication reset all**

Resetting Database Replication When You Are Reverting to an Older Product Release

If you revert the servers in a cluster to run an older product release, you must manually reset database replication within the cluster. To reset database replication after you revert all the cluster servers to the older product release, enter the CLI command **utils dbreplication reset** all on the publisher server.

When you switch versions by using Cisco Unified Communications Operating System Administration or the CLI, you get a message reminding you about the requirement to reset database replication if you are reverting to an older product release.

utils dbreplication clusterreset

This command resets database replication on an entire cluster.

Command Syntax

utils dbreplication clusterreset

Usage Guidelines

Before you run this command, run the command utils dbreplication stop first on all subscribers servers, and then on the publisher server.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils dbreplication dropadmindb

This command drops the Informix syscdr database on any server in the cluster.

Command Syntax

utils dbreplication dropadmindb

Usage Guidelines

You should run this command only if database replication reset or cluster reset fails and replication cannot be restarted.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

LDAP Authentication Fails

This section describes a common issue when LDAP authentication failure occurs.

Symptom

Login fails for end users. Authentication times out before the user can log in.

Possible Cause

You misconfigured the LDAP Port in the LDAP Authentication window in Cisco Unified Communications Manager Administration.

Recommended Action

How your corporate directory is configured determines which port number to enter in the LDAP Port field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers:

Example: LDAP Port For When the LDAP Server Is Not a Global Catalog Server

- 389—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.)
- 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

Example: LDAP Port For When the LDAP Server Is a Global Catalog Server

- 3268—When SSL is not required.
- 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

Tip Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

Issues with LDAP Over SSL

This section describes a common issue when you use LDAP over SSL.

Symptom

LDAP over SSL does not work.

Possible Cause

In most cases, problems with LDAP over SSL involve invalid, wrong, or incomplete certificates (chains) on the Unified Communications Manager server.

Explanation

In some cases, you may use multiple certificates for SSL. In most cases, uploading the AD root certificate as a directory trust is the only certificate that you need to make LDAP over SSL work. However, if a different directory trust certificate is uploaded, that is, one other than a root certificate, that other certificate must be verified to a higher level certificate, such as a root certificate. In this case, a certificate chain is created because more than one extra certificate is involved. For example, you may have the following certificates in your certificate chain:

- Root Certificate—The top-level CA certificate in the trust chain which will have similar issuer and the subject name.
- Intermediate Certificate—The CA certificate that is part of the trust chain (other than the top level). This follows the hierarchy starting from root till the last intermediate.
- Leaf Certificate—The certificate issued to the service/server which is signed by the immediate intermediate.

For example, your company has two certificates and a root certificate in your certificate chain. The following example shows the contents of a certificate:

Data:

Version: 3 (0x2)
Serial Number:

- 77:a2:0f:36:7c:07:12:9c:41:a0:84:5f:c3:0c:64:64

Signature Algorithm: sha1WithRSAEncryption
Issuer: DC=com, DC=DOMAIN3, CN=jim
Validity

- Not Before: Apr 13 14:17:51 2009 GMT
- Not After: Apr 13 14:26:17 2014 GMT

Subject: DC=com, DC=DOMAIN3, CN=jim

Recommended Action

If you have a two node chain, the chain contains the root and leaf certificate. In this case, uploading the root certificate to the directory trust is all you need to do.

If you have more than a two node chain, the chain contains the root, leaf, and intermediate certificates. In this case, the root certificate and all the intermediate certificates, excluding the leaf certificate, needs to be uploaded to the directory trust.

At the highest level in the certificate chain, that is, for the root certificate, check to make sure that the Issuer field matches the Subject field. If the Issuer field and Subject field do not match, the certificate is not a root certificate; it is an intermediate certificate. In this case, identify the complete chain from root to the last intermediate certificate, and upload the complete chain to the directory trust store.

In addition, check the Validity field to ensure the certificate has not expired. If the intermediate is expired, get the new chain from the certificate authority, along with the new leaf that is signed by using the new chain. If only the leaf certificate is expired, get a new signed certificate.

Open LDAP Cannot Verify the Certificate to Connect to the LDAP Server

Symptom

End user authentication via CTI/JTAPI clients fails, but user authentication to Unified CM works.

Possible Cause

Open LDAP cannot verify the certificate to connect to the LDAP server.

Explanation

Certificates are issued with a Fully Qualified Domain Name (FQDN). The Open LDAP verification process matches the FQDN with the server that is being accessed. Because the uploaded certificate uses FQDN and the web form is using IP Address, Open LDAP cannot connect to the server.

Recommended Action

- If possible, use DNS.

  During the Certificate Signing Request (CSR) process, ensure that you provide the FQDN as part of subject CN. Using this CSR when a self signed certificate or CA certificate is obtained, the Common Name will contain the same FQDN. Hence, no issues should occur when LDAP authentication is enabled for applications, such as CTI, CTL, and so on, with the trust certificate imported to the directory-trust.

- If you are not using DNS, enter an IP Address in the LDAP Authentication Configuration window in Unified Communications Manager Administration. Then, add the following line of text in `/etc/openldap/ldap.conf`:

  TLS_REQCERT never

  You must have a remote account to update the file, which prevents the Open LDAP library from verifying that certificate from the server. However, subsequent communication still occurs over SSL.

JTAPI Subsystem Startup Problems

The JTAPI (Java Telephony API) subsystem represents a very important component of the Cisco Customer Response Solutions (CRS) platform. JTAPI communicates with the Unified Communications Manager and has responsibility for telephony call control. The CRS platform hosts telephony applications, such as Cisco Unified Auto-Attendant, Cisco IP ICD, and Cisco Unified IP-IVR. Although this section is not specific to any of these applications, keep in mind that the JTAPI subsystem is an underlying component that all of them use.

Before starting the troubleshooting process, ensure that the software versions that you are using are compatible. To verify compatibility, read the *Cisco Unified Communications Manager Release Notes* for the version of Unified Communications Manager that you are using.

To check the version of CRS, log in to AppAdmin by entering `http://servername/appadmin`, where *servername* specifies the name of the server on which CRS is installed. Find the current version in the lower-right corner of the main menu.

JTAPI Subsystem is OUT_OF_SERVICE

Symptom

The JTAPI subsystem does not start.

Possible Cause

One of the following exceptions displays in the trace file:

- MIVR-SS_TEL-4-ModuleRunTimeFailure

- MIVR-SS_TEL-1-ModuleRunTimeFailure

Related Topics

MIVR-SS_TEL-4-ModuleRunTimeFailure, on page 47
MIVR-SS_TEL-1-ModuleRunTimeFailure, on page 49

MIVR-SS_TEL-4-ModuleRunTimeFailure

Search for the **`MIVR-SS_TEL-1-ModuleRunTimeFailure`** string in the trace file. At the end of the line, an exception reason displays.

The following list gives the most common errors:

Related Topics

Unable to create provider-bad login or password, on page 47
Unable to create provider-Connection refused, on page 47
Unable to create provider-login=, on page 48
Unable to create provider-hostname, on page 48
Unable to create provider-Operation timed out, on page 49
Unable to create provider-null, on page 49

Unable to Create Provider–Bad Login or Password

Possible Cause

Administrator entered an incorrect user name or password in the JTAPI configuration.

Full Text of Error Message

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure in JTAPI subsystem:
Module=JTAPI
Subsystem,Failure Cause=7,Failure
Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- bad login or password.
%MIVR-SS_TEL-7-
EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- bad login or password.
```

Recommended Action

Verify that the user name and password are correct. Try logging into the Unified CM User window (`http://servername/ccmuser`) on the Unified CM to ensure that the Unified CM cannot authenticate correctly.

Unable to Create Provider-Connection Refused

Possible Cause

The Unified Communications Manager refused the JTAPI connection to the Unified Communications Manager.

Full Text of Error Message

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure in JTAPI subsystem:
Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl: Unable
to create provider -- Connection refused
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Connection refused
```

Recommended Action

Verify that the CTI Manager service is running in the Cisco Unified Serviceability Control Center.

Unable to Create Provider–Login=

Possible Cause

Nothing has been configured in the JTAPI configuration window.

Full Text of Error Message

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure in JTAPI subsystem:
Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- login=
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- login=
```

Recommended Action

Configure a JTAPI provider in the JTAPI configuration window on the CRS server.

Unable to Create Provider–Hostname

Possible Cause

The CRS engine cannot resolve the host name of the Unified Communications Manager.

Full Text of Error Message

```
%M%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure in JTAPI subsystem:
Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- dgrant-mcs7835.cisco.com
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- dgrant-mcs7835.cisco.com
```

Recommended Action

Verify that DNS resolution is working correctly from the CRS engine. Try using an IP address instead of the DNS name.

Unable to Create Provider–Operation Timed Out

Possible Cause

The CRS engine does not have IP connectivity with the Unified Communications Manager.

Full Text of Error Message

```
101: Mar 24 11:37:42.153 PST%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Operation timed out
102: Mar 24 11:37:42.168 PST%MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Operation timed out
```

Recommended Action

Check the IP address that is configured for the JTAPI provider on the CRS server. Check the default gateway configuration on the CRS server and the Unified Communications Manager. Make sure no IP routing problems exist. Test connectivity by pinging the Unified Communications Manager from the CRS server.

Unable to Create Provider–Null

Possible Cause

No JTAPI provider IP address or host name get configured, or the JTAPI client is not using the correct version.

Full Text of Error Message

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure in JTAPI subsystem:
Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- null
```

Recommended Action

Verify that a host name or IP address is configured in the JTAPI configuration. If the JTAPI version is incorrect, download the JTAPI client from the Unified Communications Manager Plugins window and install it on the CRS server.

MIVR-SS_TEL-1-ModuleRunTimeFailure

Symptom

This exception usually occurs when the JTAPI subsystem cannot initialize any ports.

Possible Cause

The CRS server can communicate with the Unified Communications Manager, but cannot initialize any CTI ports or CTI route points through JTAPI. This error occurs if the CTI ports and CTI route points are not associated with the JTAPI user.

Full Text of Error Message

```
255: Mar 23 10:05:35.271 PST%MIVR-SS_TEL-1-ModuleRunTimeFailure:Real-time failure
 in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_SS,Exception=null
```

Recommended Action

Check the JTAPI user on the Unified Communications Manager and verify that CTI ports and CTI route points that are configured on the CRS server associate with the user.

JTAPI Subsystem is in PARTIAL_SERVICE

Symptom

The following exception displays in the trace file:

MIVR-SS_TEL-3-UNABLE_REGISTER_CTIPORT

Possible Cause

The JTAPI subsystem cannot initialize one or more CTI ports or route points.

Full Text of Error Message

```
1683: Mar 24 11:27:51.716 PST%MIVR-SS_TEL-3-UNABLE_REGISTER_CTIPORT:
Unable to register CTI Port: CTI Port=4503,
Exception=com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.
1684: Mar 24 11:27:51.716 PST%MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.
```

Recommended Action

The message in the trace tells you which CTI port or route point cannot be initialized. Verify that this device exists in the Unified Communications Manager configuration and also associates with the JTAPI user on the Unified Communications Manager.

Security Issues

This section provides information about security-related measurements and general guidelines for troubleshooting security-related problems.

Note This section does not describe how to reset the Cisco Unified IP Phone if it has been corrupted by bad loads, security bugs, and so on. For information on resetting the phone, refer to the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* that matches the model of the phone.

For information about how to delete the CTL file from Cisco Unified IP Phone models 7960, and 7940 only, see the System Configuration Guide for Cisco Unified Communications Manager or the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* that matches the model of the phone.

Related Topics

Security Alarms, on page 51
Security Performance Monitor Counters, on page 51
Reviewing Security Log and Trace Files, on page 52
Troubleshooting Certificates, on page 53
Troubleshooting CTL Security Tokens, on page 54
Troubleshooting CAPF, on page 56
Troubleshooting Encryption for Phones and Cisco IOS MGCP Gateways, on page 57

Security Alarms

Cisco Unified Serviceability generates security-related alarms for X.509 name mismatches, authentication errors, and encryption errors. Cisco Unified Serviceability provides the alarm definitions.

Alarms may get generated on the phone for TFTP server and CTL file errors. For alarms that get generated on the phone, refer to the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* for your phone model and type (SCCP or SIP).

Security Performance Monitor Counters

Performance monitor counters monitor the number of authenticated phones that register with Unified Communications Manager, the number of authenticated calls that are completed, and the number of authenticated calls that are active at any time. The following table lists the performance counters that apply to security features.

Table 5: Security Performance Counters

Object	Counters
Unified Communications Manager	AuthenticatedCallsActive AuthenticatedCallsCompleted AuthenticatedPartiallyRegisteredPhone AuthenticatedRegisteredPhones EncryptedCallsActive EncryptedCallsCompleted EncryptedPartiallyRegisteredPhones EncryptedRegisteredPhones SIPLineServerAuthorizationChallenges SIPLineServerAuthorizationFailures SIPTrunkServerAuthenticationChallenges SIPTrunkServerAuthenticationFailures SIPTrunkApplicationAuthorization SIPTrunkApplicationAuthorizationFailures TLSConnectedSIPTrunk
SIP Stack	StatusCodes4xxIns StatusCodes4xxOuts For example: 401 Unauthorized (HTTP authentication required) 403 Forbidden 405 Method Not Allowed 407 Proxy Authentication Required
TFTP Server	BuildSignCount EncryptCount

Refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* for accessing performance monitors in RTMT, configuring perfmon logs, and for more details about counters.

The CLI command **show perf** displays performance monitoring information. For information about using the CLI interface, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Reviewing Security Log and Trace Files

Unified Communications Manager stores log and trace files in multiple directories (`cm/log`, `cm/trace`, `tomcat/logs`, `tomcat/logs/security`, and so on).

Note For devices that support encryption, the SRTP keying material does not display in the trace file.

You can use the trace collection feature of Cisco Unified Real-Time Monitoring Tool or CLI commands to find, view, and manipulate log and trace files.

Troubleshooting Certificates

The certificate management tool in Cisco Unified Communications Platform Administration allows you to display certificates, delete and regenerate certificates, monitor certificate expirations, and download and upload certificates and CTL files (for example, to upload updated CTL files to Unity). The CLI allows you to list and view self-signed and trusted certificates and to regenerate self-signed certificates.

The CLI commands **show cert**, **show web-security**, **set cert regen**, and **set web-security** allow you to manage certificates at the CLI interface; for example, **set cert regen tomcat**. For information about how to use the GUI or CLI to manage certificates, refer to Administration Guide for Cisco Unified Communications Manager and the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Troubleshooting Ciphers

The Cipher Management page has no default values. Instead, the Cipher Management feature takes effect only when you configure Ciphers.

For information about Ciphers, see Security Guide for Cisco Unified Communications Manager

This section provides information to help you troubleshoot problems with Unified Communications Manager Ciphers:

Troubleshooting DRS and CDR Functionality

Symptom

Breakage to DRS and CDR functionality.

Possible Cause

Configuring `hmac-sha2-512` in SSH MAC interface affects the DRS and CDR functionality.

Configuring Ciphers

- `aes128-gcm@openssh.com`
- `aes256-gcm@openssh.com`

in **SSH Cipher's** field or configuring only `ecdh-sha2-nistp256` algorithm in "SSH KEX" breaks the DRS and CDR functionalities.

Recommended Action

1. From Cisco Unified OS Administration, choose **Security** > **Cipher Management**
2. Remove or Delete the above mentioned ciphers if they are already configured and **Save** the settings.

3. Reboot the server for the changes to take effect.

Troubleshooting CTL Security Tokens

The section contains information about troubleshooting CTL security tokens.

If you lose all security tokens (etokens), contact Cisco TAC for further assistance.

Troubleshooting a Locked Security Token After You Consecutively Enter an Incorrect Security Token Password

Note These troubleshooting steps are not required if you manage cluster security through the CLI command set **utils ctl**.

Each security token contains a retry counter, which specifies the number of consecutive attempts to log in to the etoken Password window. The retry counter value for the security token equals 15. If the number of consecutive attempts exceeds the counter value, that is, 16 unsuccessful consecutive attempts occur, a message indicates that the security token is locked and unusable. You cannot re-enable a locked security token.

Obtain additional security token(s) and configure the CTL file, as described in the Security Guide for Cisco Unified Communications Manager. If necessary, purchase new security token(s) to configure the file.

Note After you successfully enter the password, the counter resets to zero.

Troubleshooting If You Lose One Security Token (Etoken)

Note This procedure is not required if you manage cluster security through the CLI command set **utils ctl**.

If you lose one security token, perform the following procedure:

Procedure

1. Purchase a new security token.
2. Using a token that signed the CTL file, update the CTL file by performing the following tasks:
3. Add the new token to the CTL file.
4. Delete the lost token from the CTL file.

   For more information on how to perform these tasks, see the Security Guide for Cisco Unified Communications Manager.
5. Reset all phones, as described in the Security Guide for Cisco Unified Communications Manager.

Troubleshooting If You Lose All Security Tokens (Etoken)

Perform the following procedure if you lose the security tokens and you need to update the CTL file.

Tip Perform the following procedure during a scheduled maintenance window, because you must reboot all servers in the cluster for the changes to take effect.

Procedure

Step 1 On every Unified Communications Manager, Cisco TFTP, or alternate TFTP server, verify that CTLFile.tlv exists from the OS SSH command line.

file list tftp *CTLFile.tlv*

Step 2 Delete CTLFile.tlv.

file delete tftp *CTLFile.tlv*

Step 3 Repeat step 1 and step 2 for every Cisco Unified CallManager, Cisco TFTP, and alternate TFTP server.

Step 4 Obtain at least two new security tokens.

Step 5 By using the Cisco CTL client, create the CTL File, as described in "Installing the Cisco CTL Client" and "Configuring the Cisco CTL Client".

Tip
If the clusterwide security mode is in mixed mode, the Cisco CTL client displays the message No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode. For the system to function, you must create the CTL File and set CallManager Cluster to Mixed Mode. Click OK; then, choose Set CallManager Cluster to Mixed Mode and complete the CTL file configuration.

Step 6 Reboot all the servers in the cluster.

Step 7 After you create the CTL file on all the servers and reboot all servers in the cluster, delete the CTL file from the phone, as described in "Deleting the CTL File on the Cisco Unified IP Phone".

Troubleshooting ITL Files

Symptom

Error parsing the ITL File

Possible Cause

A Corrupt **ITLFile.tlv** or **ITLEXTFile.tlv**

Recommended Action

1. From Cisco Unified OS Administration, choose **Software Upgrade** > **TFTP File Management**

2. Search for **itlfileflags.txt** and select the file.
3. Click Delete Selected to delete the selected file.
4. Restart the TFTP service.

Enter the command **show itl** in Command Line Interface to confirm ITL status after applying actions.

Troubleshooting CAPF

This section contains information about troubleshooting CAPF.

Related Topics

Troubleshooting the Authentication String on the Phone, on page 56
Troubleshooting If the Locally Significant Certificate Validation Fails, on page 56
Verifying That the CAPF Certificate Is Installed on All Servers..., on page 56
Verifying That a Locally Significant Certificate Exists on the Phone..., on page 57
Verifying That a Manufacture-Installed Certificate (MIC) Exists in the Phone, on page 57
CAPF Error Codes, on page 58

Troubleshooting the Authentication String on the Phone

If you incorrectly enter the authentication string on the phone, a message displays on the phone. Enter the correct authentication string on the phone.

Tip Verify that the phone is registered to the Unified Communications Manager. If the phone is not registered to the Unified Communications Manager, you cannot enter the authentication string on the phone.

Verify that the device security mode for the phone equals nonsecure.

Verify authentication mode in the security profile that is applied to the phone is set to By Authentication String.

CAPF limits the number of consecutive attempts in which you can enter the authentication string on the phone. If you have not entered the correct authentication string after 10 attempts, wait at least 10 minutes before you attempt to enter the correct string again.

Troubleshooting If the Locally Significant Certificate Validation Fails

On the phone, the locally significant certificate validation may fail if the certificate is not the version that CAPF issued, the certificate has expired, the CAPF certificate does not exist on all servers in the cluster, the CAPF certificate does not exist in the CAPF directory, the phone is not registered to Unified Communications Manager, and so on. If the locally significant certificate validation fails, review the SDL trace files and the CAPF trace files for errors.

Verifying That the CAPF Certificate Is Installed on All Servers in the Cluster

After you activate the Cisco Certificate Authority Proxy Function service, CAPF automatically generates a key pair and certificate that is specific for CAPF. The CAPF certificate, which the Cisco CTL client copies to all servers in the cluster, uses the.0 extension. To verify that the CAPF certificate exists, display the CAPF certificate at the Cisco Unified Communications platform GUI or use the CLI:

- In DER encoded format—CAPF.cer
- In PEM encoded format—.0 extension file that contains the same common name string as the CAPF.cer

Verifying That a Locally Significant Certificate Exists on the Phone

You can verify that the locally significant certificate is installed on the phone at the **Model Information** or Security Configuration phone menus and by viewing the LSC setting. Refer to the *Cisco Unified IP Phone Administration Guide* for your phone model and type (SCCP or SIP) for additional information.

Verifying That a Manufacture-Installed Certificate (MIC) Exists in the Phone

You can verify that a MIC exists in the phone at the **Model Information** or Security Configuration phone menus and by viewing the MIC setting. Refer to the *Cisco Unified IP Phone Administration Guide* for your phone model and type (SCCP or SIP) for additional information.

Troubleshooting Encryption for Phones and Cisco IOS MGCP Gateways

This section contains information about troubleshooting encryption for phones and Cisco IOS MGCP Gateways.

Related Topics

Using Packet Capturing, on page 57

Using Packet Capturing

Because third-party troubleshooting tools that sniff media and TCP packets do not work after you enable SRTP encryption, you must use Cisco Unified Communications Manager Assistant to perform the following tasks if a problem occurs:

- Analyze packets for messages that are exchanged between Unified Communications Manager and the device [Cisco Unified IP Phone (SCCP and SIP), Cisco IOS MGCP gateway, H.323 gateway, H.323/H.245/H.225 trunk, or SIP trunk].

Note SIP trunks do not support SRTP.

- Capture the SRTP packets between the devices.
- Extract the media encryption key material from messages and decrypt the media between the devices.

For information about using or configuring packet capturing and about analyzing captured packets for SRTP-encrypted calls (and for all other call types), see topics related to packet capture.

Tip Performing this task for several devices at the same time may cause high CPU usage and call-processing interruptions. Cisco strongly recommends that you perform this task when you can minimize call-processing interruptions.

By using the Bulk Administration Tool that is compatible with this Unified Communications Manager release, you can configure the packet capture mode for phones. For information about how to perform this task, refer to the Bulk Administration Guide for Cisco Unified Communications Manager.

Tip Performing this task in Bulk Administration Guide for Cisco Unified Communications Manager may cause high CPU usage and call-processing interruptions. Cisco strongly recommends that you perform this task when you can minimize call-processing interruptions.

Related Topics

Packet Capture, on page 11

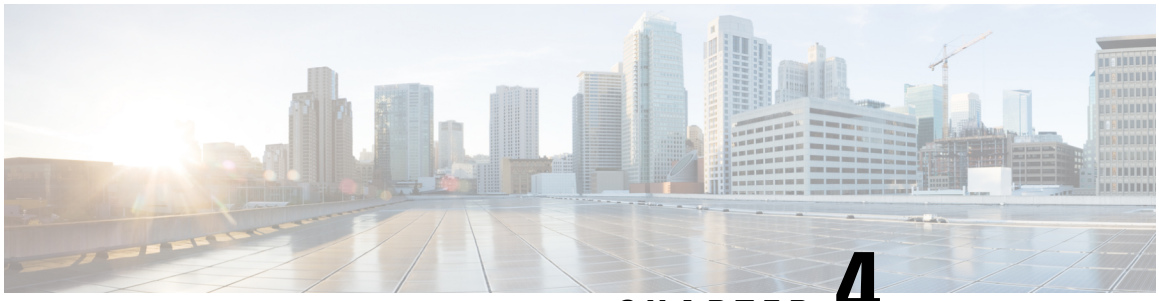
CAPF Error Codes

The following table contains CAPF error codes that may appear in CAPF log files and the corresponding corrective actions for those codes:

Table 6: CAPF Error Codes

Error Code	Description	Corrective Ac
0	CAPF_OP_SUCCESS /*Success */	No correction required.
1	CAPF_FETCH_SUCCESS_BUT_NO_CERT /* Fetch is successful; however there is no cert */	Install a certif phone. For mo information, s Guide for Cis Communicati Manager.
2	CAPF_OP_FAIL /* Fail */	No corrective available.
3	CAPF_OP_FAIL_INVALID_AUTH_STR /* Invalid Authentication string */	Enter the corr authentication phone. For mo information, s Guide for Cis Communicati Manager.
4	CAPF_OP_FAIL_INVALID_LSC /* Invalid LSC */	Update the lo significant ce (LSC) on the more informa Security Guid Unified Comm Manager.

Error Code	Description	Corrective
5	CAPF_OP_FAIL_INVALID_MIC, /* Invalid MIC */	This code the manuf certificate invalidate install a L informatic Guide for Communi Manager.
6	CAPF_OP_FAIL_INVALID_CRENDENTIALS, /* Invalid credential */	Enter corr
7	CAPF_OP_FAIL_PHONE_COMM_ERROR, /* Phone Communication Failure*/	No correc available.
8	CAPF_OP_FAIL_OP_TIMED_OUT, /* Operation timeout */	Reschedul
11	CAPF_OP_FAIL_LATE_REQUEST /* User Initiated Request Late */	Reschedul operation.



CHAPTER 4

Device Issues

This section addresses common problems that you may experience with Cisco Unified IP Phones, gateways, and related devices.

- Voice Quality, on page 61
- Codec and Region Mismatches, on page 69
- Location and Bandwidth, on page 70
- Phone Issues, on page 70
- Gateway Issues, on page 72
- Gatekeeper Issues, on page 78
- Incorrect Device Registration Status Displays, on page 80

Voice Quality

You may experience voice-quality issues including lost or distorted audio signal during phone calls. This section covers some common voice-quality problems.

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.

- Gateways
- Phones
- Networks

Related Topics

Lost or Distorted Audio, on page 62
Correcting Audio Problems from the Cisco Unified IP Phone, on page 63
Echo, on page 64
One-Way Audio or No Audio, on page 65

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 time that it takes for a packet to get from point A to point B but is simply the variation in packet arrival times.

Possible 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 reaches its destination and is ready to be put into a conventional audio stream.

The Cisco Unified IP Phone model 7960 can buffer as much as 1 second of voice samples. Because the jitter buffer is adaptive, if a burst of packets is received, the Cisco Unified IP Phone model 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).

Some video endpoints may not support G.728, and using G.728 may result in noise. Use another codec, such as G.729.

Recommended Action

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.
2. Next, disable silence suppression (also known as Voice Activation Detection or VAD). This mechanism does save bandwidth by not transmitting any audio when silence occurs, but may cause noticeable or unacceptable clipping at the beginning of words.

   Disable the service in Unified Communications Manager Administration and choose **System** > **Service Parameters**. From there, choose the server and the Cisco CallManager service.
3. Set SilenceSuppression to **False to disable for all devices in a Cisco Communications Manager cluster**; alternatively, you can set SilenceSuppressionForGateways to **False**. When in doubt, turn both off by choosing the value **False** for each.
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 following table, which represents a perfect trace, the arrival times between the audio packets (which will have an RTP header) 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. 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 Call Reporting and Billing Administration Guide for Cisco Unified Communications Manager for more information about CDRs.

Correcting Audio Problems From the Cisco Unified IP Phone

Symptom

Audio problems occur while a call is in progress.

Possible 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 that is connected to the LAN and a slow frame-relay interface that is 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 was not 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 faulty cables, interfaces, or by incorrectly configured devices (such as a port speed or duplex mismatch) cause. Make sure that the traffic is not crossing any shared-media device, such as a hub.

Recommended Action

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

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

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

- Situations could also occur where the traffic is taking a slower path through the network than expected. If QoS is configured correctly, the possibility exists that no call admission control exists. Depending on your topology, you can accomplish this through the use of **Locations** in Cisco Unified Communications Manager Administration configuration or by using a Cisco IOS router as a gatekeeper. In any case, you should always know the maximum calls that are supported across your WAN.
- Crackling represents another poor-quality symptom, which a defective power supply or some kind of strong electrical interference close to the phone sometimes causes. Try swapping the power supply and moving the phone.
- Verify gateway and phone loads. at `www.cisco.com` for the latest software loads, new patches, or release notes that relate to the problem.

After you apply the appropriate fix, verify the sound quality by performing the following procedure:

1. Test by disabling silence suppression; 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.
2. With the maximum number of calls across the WAN, the calls should all have acceptable quality.
3. Test to make sure that a fast busy is returned when you try to make one more call.

Related Topics

Lost or Distorted Audio, on page 62

Echo

Symptom

Echo occurs when the speech energy that is being generated and transmitted down the primary signal path gets coupled into the receive path from the far end. The speaker then receives 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 occurs so lowly. 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.

Possible Cause

Remember that the cause of the echo always lies 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.

Recommended Action

1. Make sure that the problem phones do not use 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

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 gets 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.

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

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 canceller cannot work properly. This issue should not exist for local calls, and long-distance calls should have external echo cancellers built in to the network at the Central Office. This fact provides one reason why you should note the external phone number of a call that experiences echo.

   Checking Your Loads

5. Verify your gateway and phone loads. Check `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 a phone call is established from an IP station through a Cisco IOS voice gateway/router, only one of the parties receives audio (one-way communication).

When a toll-bypass call is established between two Cisco gateways, only one of the parties receives audio (one-way communication).

Possible Cause

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

Recommended Action

Make Sure IP Routing is Enabled on Cisco IOS Gateway/Routers

Some Cisco IOS gateways, such as the VG200, have IP routing disabled by default. This will lead to one-way voice problems.

Note Before going any further, make sure that your router has IP routing enabled (that is, does not have the global configuration command **no ip routing**).

To enable IP routing, enter the following global configuration command in your Cisco IOS gateway:

voice-ios-gwy(config)#ip routing

Check Basic IP Routing

Ensure that basic IP access should always gets checked first. Because RTP streams have no connections (transported over UDP), traffic may travel successfully in one direction but get lost in the opposite direction.

Check the following conditions:

- Default gateways configured at the end stations
- IP routes on the default gateways, mentioned above, leading to the destination networks

Note The following list explains how to verify the default router/gateway configuration on various Cisco Unified IP Phones:

- Cisco Unified IP Phone model 7960/40—Press Settings button, select option 3, scroll down until the Default Router field shows up.

Note For Cisco DT24+ Gateways, check the DHCP Scope and make sure that a Default Gateway (003 router) option exists in the scope. The 003 router parameter populates the Default Gateway field in the devices and PCs. Scope option 3 should have the IP address of the router interface that will be doing routing for the gateway.

Bind the H.323 Signaling to a Specific IP Address on Cisco IOS Gateway/Routers

When the Cisco IOS gateway has multiple active IP interfaces, some of the H.323 signaling may use one IP address for course, and other parts of it may reference a different source addresses. This can generate various kinds of problems, including being one-way audio.

To avoid the problem, the H.323 signaling can be bound to a specific source address, which can belong to a physical or virtual interface (loopback). The command syntax to use under the interface configuration mode follows:

h323-gateway voip bind srcaddr<ip address>. Configure this command under the interface with the IP address to which the Unified Communications Manager points.

Configuring H.323 Support for Virtual Interfaces documents this command, which was introduced in Cisco IOS Release 12.1.2T.

Note A bug exists in version 12.2(6) where this solution can actually cause a one-way audio problem. For more information, refer to bug ID CSCdw69681 (registered customers only) in Cisco Software Bug Toolkit (registered customers only).

Check that Answer Supervision Is Being Sent and Received Correctly from the Telco or Switch

In an implementation that has a Cisco IOS gateway connected to a Telco or switch, verify that answer supervision gets sent correctly when the called device behind the telco or switch answers the call. Failure to receive the answer supervision will cause the Cisco IOS gateway not to cut through (open) the audio path in a forward direction which causes one-way voice. A workaround involves the need to configure **voice rtp send-recv on**.

Cut-through Two-Way Audio Early Using voice rtp send-recv on Cisco IOS Gateway/Routers

The voice path gets established in the backward direction as soon as the RTP stream is started. The forward audio path will not be cut through until the Cisco IOS gateway receives a Connect message from the remote end.

In some cases you need to establish a two-way audio path as soon as the RTP channel is opened—before the connect message is received. To achieve this, use the **voice rtp send-recv** global configuration command.

Check cRTP Settings on a Link-by-Link Basis on Cisco IOS Gateway/Routers

This issue applies to scenarios, such as toll-bypass, where more than one Cisco IOS router/gateway is involved in the voice path and Compressed RTP (cRTP) is used. cRTP, or RTP Header Compression, designates a method for making the VoIP packet headers smaller to regain bandwidth. cRTP takes the 40-byte IP/UDP/RTP header on a VoIP packet and compresses it to 2-4 bytes per packet, yielding approximately 12Kb of bandwidth for a G.729 encoded call with cRTP.

cRTP occurs on a hop-by-hop basis with decompression and recompression on every hop. Because each packet header needs to be examined for routing, enable cRTP on both sides of an IP link.

Also verify that cRTP is working as expected on both ends of the link. Cisco IOS levels vary in terms of switching paths and concurrent cRTP support.

In summary, the history follows:

- Until Cisco IOS Software Release 12.0.5T, cRTP gets process-switched.
- Cisco IOS Software Release 12.0.7T, fast- and Cisco express forwarding (CEF)-switching support for cRTP, which introduced and continue in 12.1.1T.
- In Cisco IOS Software Release 12.1.2T, introduced algorithmic performance improvements.

If you are running cRTP on Cisco IOS platforms (IOS Release 12.1), verify that bug CSCds08210 (registered customers only) (VoIP and FAX not working with RTP header compression ON) does not affect your IOS version.

Verify Minimum Software Level for NAT on Cisco IOS Gateway/Routers

If you are using Network Address Translation (NAT), you must meet the minimum software level requirements. Earlier versions of NAT do not support skinny protocol translation and will lead to one-way voice issues.

The minimum software levels that are required for using NAT and skinny simultaneously specify Cisco IOS® Software 12.1(5)T for IOS gateways to support skinny and H.323v2 with NAT.

Note If your Unified Communications Manager is using a TCP port for skinny signaling that differs from the default 2000, you need to adjust the NAT router with the **ip nat service skinny tcp port<number>** global configuration command.

The minimum software level that is required for using NAT and skinny simultaneously on a PIX firewall specifies 6.0.

Note These levels of software do not necessarily support all the RAS messages necessary for full gatekeeper support. Gatekeeper support occurs outside the scope of this document.

Disable voice-fastpath on AS5350 and AS5400

The Cisco IOS command **voice-fastpath enable** gets a hidden global configuration command for the AS5350 and AS5400, which is enabled by default. To disable it, use the **no voice-fastpath enable** global configuration command.

When enabled, this command caches the IP address and UDP port number information for the logical channel that is opened for a specific call and prevents the RTP stream from getting to the application layer, but rather forwards the packets at a lower layer. This helps marginally reduce CPU utilization in high-call-volume scenarios.

When supplementary services, such as hold or transfer are used, the voice-fastpath command causes the router to stream the audio to the cached IP address and UDP port, disregarding the new logical channel information that was generated after a call on hold was resumed or a transfer was completed. To avoid this problem, traffic should go to the application layer constantly, so redefinition of the logical channel gets taken into account, and audio gets streamed to the new IP address/UDP port pair. That explains why you should disable voice-fastpath to support supplementary services.

Configure the VPN IP Address with SoftPhone

Cisco IP SoftPhone offers the ability to make a PC work like a Cisco Unified IP Phone model 7900 Series phone. Remote users who connect back to their company network through VPN need to configure some additional settings to avoid a one-way voice problem.

The solution requires you to configure the VPN IP address, instead of the IP address of the network adapter under the Network Audio Settings.

Verification

A useful command to verify packet flow specifies **debug cch323 rtp**. This command displays packets that the router transmits (X) and receives (R). An uppercase character indicates successful transmission/reception whereas a lowercase character indicates a dropped packet. See the following example:

```
voice-ios-gwy#debug cch323 rtp
RTP packet tracing is enabled
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
```

```
!--- This is an unanswered outgoing call.
!--- Notice that voice path only cuts through in forward
!--- direction and that packets are dropped. Indeed,
!--- received packets are traffic from the IP phone to the PSTN
!--- phone. These will be dropped until the call is answered.

Mar 3 23:46:23.690: ****** cut through in FORWARD direction *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXXrrrrrrrrrrrrrrrr
voice-ios-gwy#
voice-ios-gwy#

!--- This is an example of an answered call:

voice-ios-gwy#
voice-ios-gwy#
*Mar 3 23:53:26.570: ****** cut through in FORWARD direction *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XXrrrrrXrXrXrXrXrXrXrXrXrXrXrXrrXXrrXrXrXrXrXrXXXXXXXXXXXXXXXXXrXXXXXXXXrXrXrXXrrXr
XrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr

!-- At this point the remote end picks up the phone.

*Mar 3 23:53:30.378: ****** cut through in BOTH direction *****
XRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXR
XXRRXRXRXXRRXRXRXRXRXXRXRXRXRXRXRRXRXXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XXRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXXRRRXR

!-- End of conversation.
```

Codec and Region Mismatches

If a user gets a reorder tone (busy signal) when going off hook, it could occur as 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 The system does not support codec negotiation with a Cisco IOS router.

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 Unified IP Phone model 7960—G.711A-law/mu-law, G.729, G729A, G.729Annex-B
- Cisco Access Gateway DE30 and DT-24+—G.711a-law/mu-law, G.723.1

Location and Bandwidth

If a user receives a reorder tone after dialing a number, this indicates that the cause may be that the Unified Communications Manager bandwidth allocation for the location of one of the call end devices was exceeded. Unified Communications Manager checks for the available bandwidth for each device before making a call. If no bandwidth is available, Unified Communications Managerwill not set up the call, and the user receives a reorder tone.

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

After the call is established, the Unified Communications Manager will subtract bandwidth from the locations, depending on the codec that is used in that call.

- If the call is using G.711, Unified Communications Manager subtracts 80k.
- If the call is using G.723, Unified Communications Manager subtracts 24k.
- If the call is using G.729, Unified Communications Manager subtracts 24k.

Phone Issues

This section addresses phone issues.

Related Topics

Phone Resets, on page 70
Dropped Calls, on page 71
Phones Not Registering, on page 72

Phone Resets

Symptom

Phone resets.

Possible Cause

Phones will power cycle or reset for two reasons:

- TCP failure while connecting to the Unified Communications Manager
- Failure to receive an acknowledgment to the phone KeepAlive messages.

Recommended Action

1. Check the phones and gateways to ensure that you are using the latest software loads.
2. Check `www.cisco.com` for the latest software loads, new patches, or release notes that may relate to the problem.
3. Check the Syslog Viewer in the Cisco Unified Real-Time Monitoring Tool for instances of phone(s) resetting. Phone resets represent Information events.
4. Look for any errors that may have occurred around the time that the phone(s) reset.
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

   Whether the resets occur during a call or happen intermittently

   Whether any similarities of phone model exist
6. Start a Sniffer trace on a phone that frequently resets. After the phone has reset, look at the trace to determine whether any TCP retries are 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 that DHCP lease expiration occurs every seven days (this value is user-configurable; for example, it could be every 2 minutes).

Dropped Calls

Symptom

Premature termination of dropped calls.

Possible Cause

Premature termination of dropped calls can result from a phone or gateway resetting or a circuit problem, such as incorrect PRI configuration.

Recommended Action

1. Determine whether this problem is isolated to one phone or to a group of phones. Perhaps you will find that the affected phones all exist on a particular subnet or location.
2. Check the Syslog Viewer in the *Cisco Unified Real-Time Monitoring Tool* (RTMT) 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 Unified Communications Manager alive, so the Unified

Communications Manager 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 Performance Monitoring in RTMT.

3. If the problem seems to be occurring only through a certain gateway, 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. See *CDR Analysis and Reporting Administration Guide* for detailed information on CDRs.
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/en/US/tech/tk801/tk379/technologies_tech_note09186a008012e95f.shtml
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 Unified Communications Manager. Because the trace tool can affect Unified Communications Manager performance, you will want to use this option only as a last resort or if your network is not yet in production.

Related Topics

Phone Resets, on page 70

Phones Not Registering

Symptom

Cannot register more than 5000 phones.

Possible Cause

The Maximum Number of Registered Devices service parameter specifies the default value.

Recommended Action

Change the value of the Maximum Number of Registered Devices service parameter on each node to the appropriate value.

Gateway Issues

This section addresses gateway issues.

Related Topics

Gateway Reorder Tone, on page 72
Gateway Registration Failure, on page 73

Gateway Reorder Tone

Symptom

Reorder tone occurs.

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

Recommended Action

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

1. Check the gateways to ensure that you are using the latest software loads.
2. Check `www.cisco.com` for the latest software loads, new patches, or release notes relating to the problem.
3. Start an SDI trace and re-create the problem. Reorder tones result from a configuration issue with location-based admission control or gatekeeper-based admission control where the Unified Communications Manager might limit the number of allowable calls. In the SDI trace, locate the call to determine whether it was blocked intentionally by a route pattern or the calling search space or by any other configuration setting.
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 standalone units that do not directly connect to a Network Management Processor (NMP). The second category includes the Analog Access WS-X6624 and Digital Access WS-X6608. These gateways, as blades that are installed in a Catalyst 6000 chassis, provide direct connectivity to the NMP for control and statusing.

Symptom

A registration problem represents one of the most common issues that is encountered with gateways on a Unified Communications Manager.

Possible Cause

Registration can fail for a variety of reasons.

Recommended Action

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, this indicates that the gateway software is not running. Normally, this results in an automatic reset of the gateway. Also, consider it as 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 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 displays 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 eight 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.

2. Check that the gateway received its IP address. A standalone gateway must receive its IP address using DHCP or BOOTP. A Catalyst gateway may receive its IP address by DHCP, BOOTP or by manual configuration through the NMP.
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 a definitive indication. Delete the lease at the DHCP server.
4. Reset the gateway.
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?).
6. If performing these checks does not yield the answer, use a sniffer trace to determine the specific problem.
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
```

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.
9. If the gateway is failing to obtain valid DHCP information, use the tracy utility (supplied by Cisco TAC) to determine the problem.
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. Issue the command **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.

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.

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.

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*

14. If you are still seeing the **DHCPState = INIT** messages, check whether the DHCP server is functioning correctly.

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.

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.

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 using 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.

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: 0Cmd:    show tl
```

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, bold lines of text make it easier for you to see the messages that are 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: 6Cmd:     show dhcp
```

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

20. After 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 Unified Communications Manager:

```
00:09:05.620 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP
Server00:09:18.620 (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 Unified Communications Manager.

21. If the card is not getting its TFTP information correctly, check the TFTP service on the Unified Communications Managerand make sure it is running.

22. Check the TFTP trace on the Unified Communications Manager.

Another common problem occurs if the gateway is not configured correctly on the Unified Communications Manager. 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
asynchronously2000 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 CM 10.123.9.2
00:00:05.610 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupUnified CM
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 CM 10.123.9.2
00:00:20.600 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
```

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 =
SentRegister00:00:08.010 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 display.

```
ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE00:00:00.050 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 CM 10.123.9.2
00:00:05.730 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
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 = BadUnified CM
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 CM 10.123.9.2
00:01:51.300 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
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: Unified CM#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 Unified Communications Manager Administration.

Gatekeeper Issues

Before starting any gatekeeper troubleshooting, verify that IP connectivity exists within the network. Assuming that IP connectivity exists, proceed to troubleshoot your gatekeeper calls.

Related Topics

Admission Rejects, on page 78
Registration Rejects, on page 79

Admission Rejects

Symptom

The system issues Admission Rejects (ARJ) when Unified Communications Manager has registered with the gatekeeper but cannot send a phone call.

Possible Cause

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

Recommended Action

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

5. Verify the bandwidth configuration.

Registration Rejects

Symptom

The system issues Registration Rejects (RRJ) when Unified Communications Manager cannot register with the gatekeeper.

Possible Cause

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

Recommended Action

1. Verify IP connectivity from the Unified Communications Manager to the gatekeeper.
2. Show gatekeeper status and verify that the gatekeeper state is up.
3. Is a zone subnet defined on the gatekeeper? If so, verify that the subnet of the gateway is in the allowed subnets.

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

Symptom

When the Unified Communications Manager 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.

Possible 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 Unified Communications Manager server, the Unified Communications Manager 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 MGCP backhaul on the 2600/3600) is used.

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

You see this happening frequently 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.

Recommended Action

Reset the E1 port.

Verification

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

Incorrect Device Registration Status Displays

Symptom

Incorrect device registration status displays in the device windows in Unified Communications Manager Administration.

Possible Cause

Cisco RIS Data Collector service provides the current device registration status to Unified Communications Manager Administration windows. If the status does not display, one of the following causes may exist:

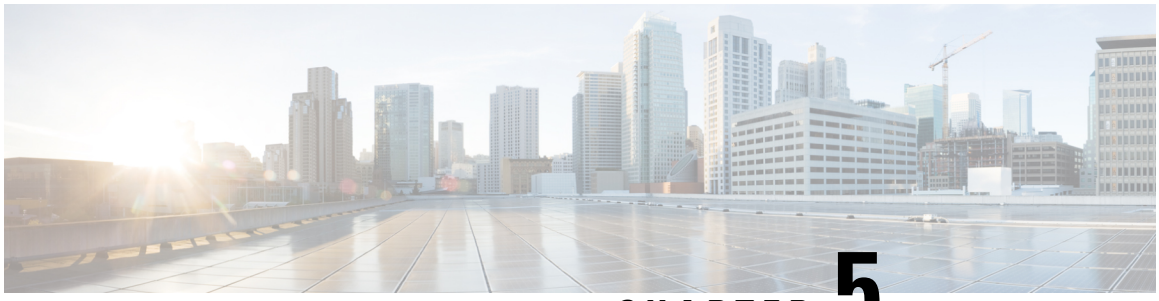
The Cisco RIS Data Collector service is not running or not responding.

Network connectivity issues or DNS name resolution issues exist, so Unified Communications Manager Administration cannot establish communication with the Cisco RIS Data Collector service.

Recommended Action

1. Using Cisco Unified Serviceability, make sure that the Cisco RIS Data Collector service is running. If the service is running, restart the service. For information on checking service status and restarting services, refer to the *Cisco Unified Serviceability Administration Guide*.
2. Ensure that:
   - The DNS server is properly configured and available
   - The hosts file has proper mapping for Unified Communications Manager servers
   - No DNS resolution issues exist for Unified Communications Manager servers in the cluster
   - You add local server name to the hosts file and perform ipconfig /flushdns, ipconfig /registerdns, iisrest.

Note To verify DNS resolution, make sure that the nslookup tool can resolve the hostnames of servers in the cluster.



CHAPTER 5

Dial Plans and Routing Issues

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

- Route Partitions and Calling Search Spaces, on page 81
- Group Pickup Configuration, on page 83
- Dial Plan Issues, on page 83
- Automated Alternate Routing (AAR) Limitation with Remote Gateways, on page 85

Route Partitions and Calling Search Spaces

Route partitions inherit the error-handling capabilities for the Unified Communications Manager software. This means that 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 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 System Configuration Guide for Cisco Unified Communications Manager 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 CCM Communications Manager|StationInit - InboundStim -
OffHookMessageID tcpHandle=0x6b8802808:38:54.968 CCM CallManager|StationD -
stationOutputDisplayText tcpHandle=0x6b88028, Display= 5000
08:38:54.968 CCM CallManager|StationD - stationOutputSetLamp stim: 9=Line
instance=1 lampMode=LampOn tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputCallState tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputActivateCallPlane
tcpHandle=0x6b88028
08:38:54.968 CCM 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 that is 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 CCM CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist08:38:54.968 CCM CallManager|StationD -
stationOutputStartTone: 33=InsideDialTone tcpHandle=0x6b88028
08:38:55.671 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 5 tcpHandle=0x6b88028
08:38:55.671 CCM CallManager|StationD - stationOutputStopTone tcpHandle=0x6b88028
08:38:55.671 CCM CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:55.671 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5")
08:38:55.671 CCM CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:56.015 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x6b88028
08:38:56.015 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="50")
08:38:56.015 CCM CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:56.187 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x6b88028
08:38:56.187 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="500")
08:38:56.187 CCM CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:56.515 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 3 tcpHandle=0x6b88028
08:38:56.515 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5003")
08:38:56.515 CCM CallManager|Digit analysis: analysis results
08:38:56.515 CCM CallManager||PretransformCallingPartyNumber=5000
```

Be aware 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 Unified Communications Manager is attempting to dial the directory number 1001 and it is not in the Calling Search Space for that device. Again, be aware that the digit analysis routine had potential matches until only the first digit was dialed. The route pattern that is associated with the digit 1 resides 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 CCM CallManager|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x6b8802808:38:58.734 CCM CallManager|StationD - stationOutputDisplayText
 tcpHandle=0x6b88028, Display= 5000
08:38:58.734 CCM CallManager|StationD - stationOutputSetLamp stim: 9=Line
instance=1 lampMode=LampOn tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputCallState tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputActivateCallPlane
tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")
08:38:58.734 CCM CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:58.734 CCM CallManager|StationD - stationOutputStartTone: 33=InsideDialTone
 tcpHandle=0x6b88028
08:38:59.703 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 1 tcpHandle=0x6b88028
```

```
08:38:59.703 CCM CallManager|StationD - stationOutputStopTone tcpHandle=0x6b88028
08:38:59.703 CCM CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:59.703 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="1")
08:38:59.703 CCM CallManager|Digit analysis:
potentialMatches=NoPotentialMatchesExist
08:38:59.703 CCM 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 that is associated with the partition that is listed first in the partition search space.

Group Pickup Configuration

Symptom

Group pickup feature does not work for a group that is configured with a partition.

Possible Cause

The Calling Search Space (CSS) may not be configured correctly for each Directory Number (DN) in the group

Example

The following steps provide an example of correct group pickup configuration with partitioning:

1. Configure a pickup group named Marketing/5656, where *Marketing* is the partition and 5656 is the pickup number.
2. On the configuration for DNs 6000 and 7000, respectively, add these DNs to the pickup group that is named *Marketing/5656*.

Recommended Action

If group pickup fails, check the CSS of each domain name (DNs 6000 and 7000 in this example). If the partition that is called *Marketing* is not contained in each CSS in this example, then the configuration is incorrect and may cause a failed pickup.

Dial Plan Issues

This section addresses dial plan issues.

Related Topics

Problem When Dialing a Number, on page 84
Secure Dial Plan, on page 85

Problem When Dialing a Number

Symptom

Problems occur when a number is dialed.

Possible Cause

A Dial Plan comprises a list of numbers and groups of numbers that tell the Unified Communications Manager to what devices (such as phones and gateways) to send calls when a certain string of digits is collected. Consider this setup as analogous to a static routing table in a router.

Be sure that your dial plan concepts, basic call routing, and planning are carefully considered and properly configured before trying to troubleshoot a potential dial plan issue. Often, the problem lies with planning and configuration. Refer to the route plan configuration chapters in the System Configuration Guide for Cisco Unified Communications Manager for more information.

Recommended Action

1. Identify the Directory Number (DN) that is originating the call.
2. Identify the Calling Search Space for this DN.

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

3. If applicable, identify devices with which the Calling Search Space associates with this DN. Make sure that you identify the correct device; because multiple line appearances are supported, you can have the same DN on multiple devices. Keep track of the device calling search space.

   If this is a Cisco Unified IP Phone that is originating the call, remember that a particular line (DN) and the device with which a line is associated have calling search spaces. They will get combined when a call is made. For example, if line instance 1000 has a Calling Search Space of AccessLevelX and the Cisco Unified 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, Unified Communications Manager will search through partitions that are contained in Calling Search Space AccessLevelX and AccessLevelY.
4. Identify which Partitions associate with the Calling Search Space(s).

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

5. Identify to which Partition of the device the call should (or should not) go.
6. Identify which number is being dialed. Keep track of if and when the user is getting a secondary dial tone. Also keep track of what they receive after all the digits have been entered (reorder, fast-busy). Does the user get the progress tones before expecting to receive 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.

7. Generate a Route Plan Report in Unified Communications Manager and use it to examine all the route patterns for the partitions that are in the Calling Search Space for the problem call.
8. If necessary, add or modify the Route Patterns or Route Filters.
9. If you can find the Route Pattern to which the call is being sent, keep track of the Route List or Gateway to which the pattern points.
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.
11. Verify that the applicable devices are registered with Unified Communications Manager.
12. If a gateway has no access to Unified Communications Manager, use the show tech command to capture and verify this information.
13. Pay attention to the @ sign. This macro can expand to include many different things. It gets often used in combination with filtering options.
14. If a device is not part of a partition, consider it 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.
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 Unified 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 Unified Communications Manager 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 that you want to do when you try to fix a filtering problem is to run an SDI trace. Not enough information exists, and the potential for causing more harm is too great.

Automated Alternate Routing (AAR) Limitation with Remote Gateways

Symptom

AAR exhibits the limitation that calls routed over a remote gateway during a high-bandwidth situation fail, and the calls cannot be routed over the local gateway when AAR is used. This functionality is important to customers who use Tail-End Hop Off (TEHO) for toll bypass.

Recommended Action

The following example provides a workaround to use for calls that must be routed over a remote gateway in high-bandwidth situations when AAR is in use.

Workaround Example

Use a specific partition for the TEHO in question.

In the following example, headquarters (HQ) has area code 408 and the Branch (BR1) has area code 919.

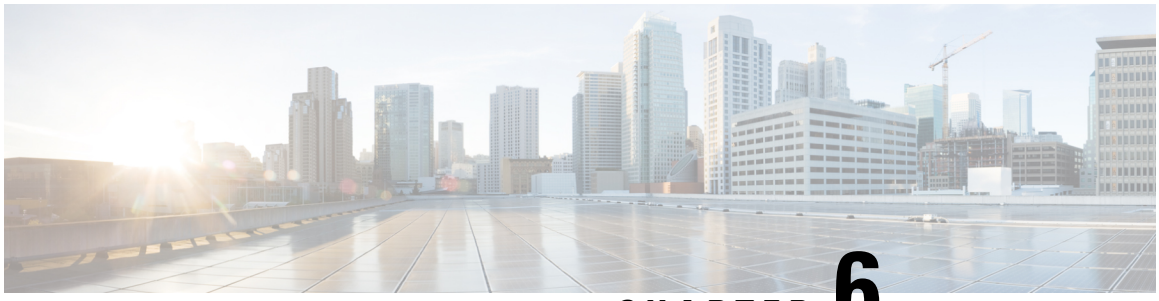
Configure as follows:

1. Create theTehoBr1forHQPt partition and assign this partition to the calling search space (CSS) of the HQ devices with a higher priority than the regular PSTN access uses.
2. Create the TehoBr1forHQRL route list and add the BR1 gateway route group to this route list as the first option and the HQ gateway as the second option.
3. Apply called party modification within the route list. In this case, apply predot called party modification for the BR1 route group, and apply predot and prefix 1919 called party modification for the HQ route group.
4. Ensure that the gateway does not perform called party modification.
5. Create a route pattern in the TehoBr1forHQPt partition.
6. Ensure that no called party modifications are applied in the route pattern.

Results

In an out-of-bandwidth situation, after Unified Communications Manager tries to allocate the first route group for TEHO (BR1 route group), Unified Communications Manager retries the second route group, at which point the system strips the 91919 string and replaces it with the 1919 string, which is suitable for long-distance dialing. Because the string is configured for use by the local gateway, less rerouting takes place.

AAR works on a per-external-phone-number-mask basis and cannot be processed for an external PSTN number because the system does not know the phone number mask of the PSTN number. This workaround provides AAR functionality and improves network resiliency.



CHAPTER 6

Cisco Unified Communications Manager Services Issues

This section covers the solutions for the most common issues that relate to Unified Communications Manager services.

- No Available Conference Bridge, on page 87
- Hardware Transcoder Not Working As Expected, on page 89
- No Supplementary Services Are Available on an Established Call, on page 90

No Available Conference Bridge

Symptom

The following message displays: No Conference Bridge Available.

Possible Cause

This could indicate either a software or a hardware problem.

Recommended Action

1. Check to see whether you have any available software or hardware conference bridge resources that are registered with Unified Communications Manager.
2. Use the Unified Communications Manager Cisco Unified Real-Time Monitoring Tool to check the number of Unicast AvailableConferences.

   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 (three people/conference), as shown in the following trace.

Note The number of supported devices may vary with different Unified Communications Manager releases. Refer to the appropriate version of Unified Communications Managerdocumentation at the following location:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

```
10:59:29.951 CCM CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB_kirribilli - Registered -
ConfBridges= 16, Streams= 48, tcpHandle=4f12738 10:59:29.951 CCM
CallManager|UnicastBridgeManager - UnicastBridgeRegistrationReq - Device
Registration Complete for Name= Xoð ô%ð  - 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 CCM CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB00107B000FB0 - Registered -
ConfBridges= 5, Streams= 16, tcpHandle=4f19d64 11:14:05.480 CCM
CallManager|UnicastBridgeManager - UnicastBridgeRegistrationReq - Device
Registration Complete for Name= Xoð ô%ð  - 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 registered as a Conference Bridge with Unified Communications Manager.

```
greece-sup (enable) sh port 4/1Port  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
```

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.
4. Check the setting of the Audio Bandwidth field on the Location Configuration window. If the call bandwidth exceeds this configured limit, the conferencing fails. To resolve this issue, choose the Unlimited Bandwidth radio button. For more information on the Location Configuration window, refer to the System Configuration Guide for Cisco Unified Communications Manager.

Hardware Transcoder Not Working As Expected

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).

Possible Cause

You may not have any available transcoder resources that are registered with Unified Communications Manager (must be hardware).

Recommended Action

Use the Unified Communications Manager Cisco Unified Real-Time Monitoring Tool to check the number of available resources by viewing the ResourceAvailable counter in the Cisco MTP Device object.

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 Unified Communications Manager releases. Refer to the appropriate version of Unified Communications Manager documentation at the following location: *http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html*

```
11:51:09.939 CCM 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 registered as an MTP/transcoder with Unified Communications Manager.

```
greece-sup (enable) sh port 4/2Port  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 Unified Communications Manager 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, Unified Communications Manager realizes it is a Cisco Unified IP Phone model 7960, which supports G.729. After the digits are collected, the Unified Communications Manager 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, initiates a call to Phone D, this time the Unified Communications Manager would realize that the originating phone only supports G.723 or G.711. Unified Communications Manager 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, 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.

No Supplementary Services Are Available on an Established Call

Symptom

A call gets established, but supplementary services are not available.

Possible 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.

Recommended Action

1. Determine whether you have any available software or hardware MTP resources that are registered with Unified Communications Manager.
2. Use Performance monitoring in theUnified Communications Manager Cisco Unified Real-Time Monitoring Tool to check the number of MTP devices available.

   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 Unified Communications Manager releases. Refer to the appropriate version of Unified Communications Manager documentation at the following location:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

```
10:12:19.161 CCM CallManager|MediaTerminationPointControl - Capabilities
Received - Device= MTP_kirribilli. - Registered - Supports 24 calls
```

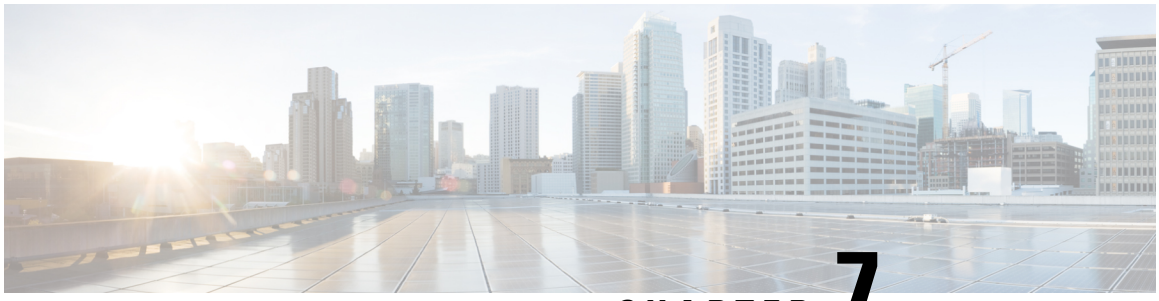
One E1 port (WS-X6608-E1 card contains 8x E1 ports) provides MTP resources for 16 calls, as shown in the following trace.

```
11:51:09.939 CCM 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 Unified Communications Manager.

```
greece-sup (enable) sh port 4/2Port  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
```

3. In the Gateway Configuration window of Cisco Unified Communications Manager Administration , check to see whether the **Media Termination Point Required** check box is checked.
4. Verify that Unified Communications Manager allocated the required number of MTP devices.



CHAPTER 7

Voice Messaging Issues

This section covers the solutions for the most common voice-messaging issues.

For extensive troubleshooting information for Cisco Unity voice messaging, refer to the *Cisco Unity Troubleshooting Guide* at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html

For all documentation that relates to Cisco Unity systems, refer to the following URL:
http://www.cisco.com/en/us/products/sw/voicesw/ps2237/tsd_products_support_series_home.html

- Voice Messaging Stops After 30 Seconds, on page 93
- Cisco Unity System Does Not Roll Over: Receive Busy Tone, on page 94
- Calls That Are Forwarded to Voice Messaging System Get Treated as a Direct Call to Cisco Unity System, on page 94
- Administrator Account Is Not Associated with Cisco Unity Subscriber, on page 95

Voice Messaging Stops After 30 Seconds

Symptom

When Cisco Unity system is running with Unified Communications Manager, a caller gets only 30 seconds in which to leave a voice-mail message.

Possible Cause

This problem occurs when a caller is leaving a voice message and the call terminates 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.

Recommended Action

1. To resolve this problem, verify that the Media Gateway Control Protocol (MGCP) is being used on the voice gateway.
2. If the MGCP is being used, add the **no mgcp timer receive-rtcp** command.
3. If MGCP is not on the voice gateway, enable Skinny traces for the Cisco Unity server and Cisco Communications Manager traces.

For information on setting Cisco Unity diagnostic traces, refer to the "Diagnostic Trace Utilities and Logs" section of the applicable *Cisco Unity Troubleshooting Guide* at *http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html*

Cisco Unity System Does Not Roll Over: Receive Busy Tone

Symptom

Cisco Unity Connection system does not get past the first line and will not roll over to the second port.

Example

```
Call 5000 from 1001Get Unity
Place the call on Hold
Press New Call
Dial 5000
Get Busy tone
Press End Call
Press Resume Call
Press End Call
```

Possible Cause

The *Cisco Messaging Interface* (CMI) service is configured with the same number as Cisco Unity Connection (5000), and it is registering the intercept, so the call is hitting the CMI.

Recommended Action

Check the CMI service parameters to ensure that the voicemaildn parameter is not configured.

Calls That Are Forwarded to Voice Messaging System Get Treated as a Direct Call to Cisco Unity System

Symptom

Calls from one Cisco Unified IP Phone to another that are forwarded to voice-messaging system get treated as a direct call to Cisco Unity Connection system from the phone that is making the call. However, this only occurs if the digits are dialed but works properly (receiving the called-phone greeting) if the Redial softkey is pressed.

Possible Cause

The logic in the TSP states that if the call is a forwarded call and the originalCalledPartyName is "Voicemail," mark the call as a direct call. This was done for failover Cisco Unity Connection systems that are using Unified Communications Manager.

Recommended Action

1. On the Unified Communications Manager server, change the name of the Display field on the Cisco Voice Mail ports to anything other than "VoiceMail."
2. On the Cisco Unity Connection server, add a new Registry string value of HKLM\Software\ActiveVoice\AvSkinny\voiceMail display Name= anything other than VoiceMail.

Administrator Account Is Not Associated with Cisco Unity Subscriber

Symptom

While attempting to access the System Administrator (SA) page, you receive a message stating that the administrator account is not associated with the *Cisco Unity* subscriber.

Possible Cause

Access was not configured for the user.

Recommended Action

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 the "Granting Administrative Rights to Other Cisco Unity" section of the "Accessing the Cisco Unity Administrator" chapter in the applicable *Cisco Unity System Administration Guide* at *http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html*

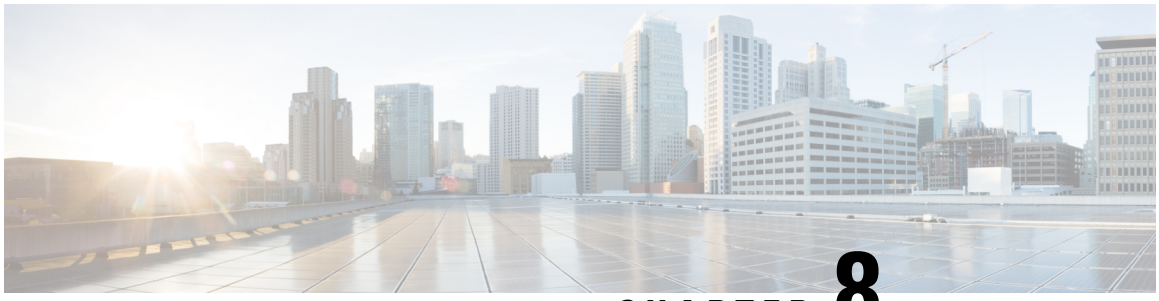
Note For more information about the GrantUnityAccess utility, see *Granting Administrative Rights to Other Cisco Unity Servers* at the following URL: *http://www.cisco.com/en/US/docs/voice_ip_comm/unity/3x/administration/guide/312/SAG_0255.html#wp1060485*

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.



CHAPTER 8

Troubleshooting Features and Services

This chapter provides information to help you resolve common issues with Unified Communications Manager features and services.

- Troubleshooting Barge, on page 97
- Troubleshooting Call Back, on page 98
- Troubleshooting Call Control Discovery, on page 100
- Troubleshooting Call Park, on page 102
- Troubleshooting Ciphers, on page 103
- Troubleshooting Cisco Extension Mobility, on page 103
- Troubleshooting Cisco Unified Communications Manager Assistant, on page 106
- Troubleshooting Cisco Unified Mobility, on page 115
- Troubleshooting Cisco Web Dialer, on page 116
- Troubleshooting Directed Call Park, on page 119
- Troubleshooting External Call Control, on page 121
- Troubleshooting Hotline, on page 124
- Troubleshooting Immediate Divert, on page 125
- Troubleshooting Intercom, on page 126
- Troubleshooting IPv6, on page 128
- Troubleshooting Logical Partitioning, on page 130
- Troubleshooting SIP with DNS Caching Enabled, on page 133
- Troubleshooting SAML Single Sign On, on page 137

Troubleshooting Barge

This section covers the solution for the most common issue that is related to the Barge feature.

Symptom

When the Barge softkey is pressed, the message No Conference Bridge Available displays on the IP phone.

Possible Cause

Built in Bridge setting in Phone Configuration for the target phone did not get set properly.

Corrective Action

To resolve the problem, perform the following steps:

Procedure

1. From Unified Communications Manager Administration, go to **Device** > **Phone** and click **Find the phone** to find the phone configuration of the phone that is having the problem.
2. Set the Built In Bridge parameter to **On**.
3. Click Update.
4. Reset the phone.

Troubleshooting Call Back

This section provides symptoms, possible causes, recommended actions, and error messages when Call Back does not work as expected.

Related Topics

Error Messages for Call Back, on page 100
Locating the Call Back Log Files, on page 100
Problems Using Call Back, on page 98

Problems Using Call Back

This section describes problems, possible causes, recommended actions, and error messages, if applicable to the problem.

User presses Callback softkey before phone rings

Symptom

During a call, the CallBack softkey may display on the phone, even though the phone is not ringing yet.

Possible Cause

User may not be pressing the CallBack softkey at the appropriate time.

Corrective Action

Users must press the CallBack softkey after a ringing or busy signal is received. Pressing the softkey at the wrong time may cause an error message to display on the phone.

User unplugs or resets phone after pressing the CallBack softkey but before Call Back occurs

Symptom #1

Caller phone reset occurs after CallBack softkey is pressed but before Call Back is activated.

Possible Cause

The user reset the phone.

Corrective Action #1

The caller phone does not display the Call Back activation window after the reset, and the caller must press the CallBack softkey to view the active Call Back service. Call Back notification occurs on the phone.

Symptom #2

Caller phone reset occurs after Call Back is activated but before called party becomes available.

Possible Cause

The user reset the phone.

Corrective Action #2

You do not need to perform a corrective action. If the reset occurs before the called party becomes available, Call Back occurs as expected.

Symptom #3

Caller phone reset occurs after Call Back is activated, but called party becomes available before the reset completes on the caller phone.

Possible Cause

The user reset the phone.

Corrective Action #3

CallBack notification does not occur automatically, so the caller must press the CallBack softkey to view the active Call Back service.

Caller misses availability notification before phone reset. Replace/retain screen does not explicitly state that availability notification occurred.

Symptom

In an intracluster or intercluster call back scenario, a caller initiates Call Back for a user, for example, user B, who is unavailable. When user B becomes available, the availability notification screen displays on the caller phone, and a tone plays. The caller misses the availability notification for some reason, and the phone resets.

The caller contacts a different user, user C, for example, and presses the CallBack softkey because user C appears busy. The replace/retain screen displays on the caller phone, but the screen does not state that the availability notification already occurred for user B.

Possible Cause

The user reset the phone.

Corrective Action

After a phone reset but not during an active call, review the call back notifications on the phone. Press the CallBack softkey.

Error Messages for Call Back

This section provides a list of error messages that may display on the phone.

Error Message `Call Back is not active. Press Exit to quit this screen.`

Explanation User presses the CallBack softkey during the idle state.

Recommended Action The error message provides the recommended action.

Error Message `CallBack is already active on xxxx. Press OK to activate on yyyy. Press Exit to quit this screen.`

Explanation A user tried to activate Call Back, but it is already active.

Recommended Action The error message provides the recommended action.

Error Message `CallBack cannot be activated for xxxx.`

Explanation A user tried to activate Call Back, and the extension is not found in the database.

Recommended Action The user must try again, or the administrator must add the directory number to Unified Communications Manager Administration.

Error Message `Service is not active.`

Explanation You set the Callback Enabled Flag service parameter to **False**, which means that the feature remains disabled.

Recommended Action For the Call Back feature, configure the Cisco CallManager service parameter, Callback Enabled Flag, to **True**.

Locating the Call Back Log Files

Traces for the Call Back feature exist as Unified Communications Manager and CTIManager SDL and SDI records. To access the traces, refer to the *Cisco Unified Serviceability Administration Guide*.

Troubleshooting Call Control Discovery

The following alarms support the call control discovery feature. To access the alarm definitions in Cisco Unified Serviceability, choose **Alarm** > **Definitions**. The alarms support the CallManager alarm catalog (choose **CallManager Alarm Catalog** > **CallManager**).

- SAFUnknownService
  - Informational alarm
  - Unified Communications Manager does not recognize the service ID in a publish revoke or withdrawal message that the SAF forwarder issued.
- SAFPublishRevoke
  - Informational alarm

- You issued a CLI command on the SAF Forwarder router to revoke the publish action for the service or subservice ID that is specified in this alarm.

- DuplicateLearnedPattern
  - Error alarm
  - The call control discovery requesting service received the same hosted DN from multiple remote call-control entities. The parameter, Issue Alarm for Duplicate Learned Patterns, controls whether this alarm gets issued.
  - In RTMT, open the Learned Pattern report and find the duplicate pattern that is specified in this alarm. Ensure that the learned patterns are unique. Determine which remote call-control entity needs to be changed so duplicate patterns do not exist.

- CCDIPReachableTimeOut
  - Error Alarm
  - The CCD requesting service detected that it can no longer reach the learned patterns through IP. All learned patterns from this SAF forwarder get marked as unreachable (via IP), and all calls to learned patterns get routed through the PSTN. Calls get routed through the PSTN for a specific amount of time before PSTN failover times out.
  - Check IP connectivity and resolve any TCP or IP problems in the network.

- CCDPSTNFailOverDurationTimeOut
  - Error Alarm
  - When learned patterns are not reachable through IP, Unified Communications Manager routes calls through the PSTN. When this alarm occurs, the PSTN failover duration has expired, and calls to learned patterns cannot be routed. All learned patterns get purged from Unified Communications Manager.
  - Troubleshoot your network to get IP connectivity restored. After IP connectivity is restored, Unified Communications Manager automatically relearns patterns and calls to learned patterns automatically proceed through IP.

- CCDLearnedPatternLimitReached
  - Warning Alarm
  - This alarm indicates that the CCD requesting service has met the maximum number of allowed learned patterns.
  - This alarm displays the value that is configured for the parameter, CCD Maximum Numbers of Learned Patterns, as well as the maximum number of learned patterns that are allowed by the system (20,000). Consider whether the specified maximum number of learned patterns is correct for your deployment. If the value is too low, compare it with the number that displays in the SystemLimitCCDLearnedPatterns in this alarm. If the maximum number is below the system limit, which is 20,000 learned patterns, increase the value for the CCD Maximum Numbers of Learned Patterns parameter.

- LostConnectionToSAFForwarder

- Error alarm
- A TCP connection failure caused the connection between the SAF forwarder and Unified Communications Manager to be lost. When the TCP connection is restored, Unified Communications Manager attempts to connect to the SAF forwarder automatically. If IP connectivity is unreachable for longer than the duration of the CCDLearnedPatternIPReachableDuration feature parameter, calls to learned patterns get routed through PSTN instead of through IP. Calls through PSTN to learned patterns get maintained for a specific period of time before PSTN failover times out.
- Investigate possible causes of a TCP connection failure, such as power failure, loose cables, incorrect switch configuration, and so on.

- SAFForwarderError
  - Unified Communications Manager received an error from the SAF forwarder.
  - Refer to the reason code and description for specific information and actions (where applicable) about the reason that this alarm occurred.

    For example, reason code 472 indicates that the external client, in this case, Unified Communications Manager, did not increment the service version number correctly. For example, reason code 474 indicates that the external client, in this case, Unified Communications Manager, sent a publishing request over a TCP connection to the SAF forwarder before the client registers to the forwarder. For example, reason code 400 indicates that the external client, in this case, Unified Communications Manager, did not construct the SAF message correctly.

Troubleshooting Call Park

The following table provides troubleshooting recovery tips for common call park problems.

Table 7: Troubleshooting Tips for Call Park

Problem Description	Recommended Action
User cannot park calls. When the user presses the Park softkey or feature button, the call does not get parked.	Ensure that a unique call park number is assigned to each Unified Communications Manager in the cluster. See the System Configuration Guide for Cisco Unified Communications Manager. The partition that is assigned to the call park number does not match the partition that is assigned to the phone directory number. See the System Configuration Guide for Cisco Unified Communications Manager.
The call park number does not display long enough for the user.	Set the Call Park Display Timer to a longer duration. For information on setting parameters for call park, see the System Configuration Guide for Cisco Unified Communications Manager.

Troubleshooting Ciphers

The Cipher Management page has no default values. Instead, the Cipher Management feature takes effect only when you configure Ciphers.

For information about Ciphers, see Security Guide for Cisco Unified Communications Manager

This section provides information to help you troubleshoot problems with Unified Communications Manager Ciphers:

Troubleshooting DRS and CDR Functionality

Symptom

Breakage to DRS and CDR functionality.

Possible Cause

Configuring `hmac-sha2-512` in SSH MAC interface affects the DRS and CDR functionality.

Configuring Ciphers

- `aes128-gcm@openssh.com`
- `aes256-gcm@openssh.com`

in **SSH Cipher's** field or configuring only `ecdh-sha2-nistp256` algorithm in "SSH KEX" breaks the DRS and CDR functionalities.

Recommended Action

1. From Cisco Unified OS Administration, choose **Security** > **Cipher Management**
2. Remove or Delete the above mentioned ciphers if they are already configured and **Save** the settings.
3. Reboot the server for the changes to take effect.

Troubleshooting Cisco Extension Mobility

Cisco Extension Mobility provides troubleshooting tools for the administrator. These tools include performance counters (also known as perfmons) and alarms that are part of Cisco Unified Serviceability. For information about performance counters (perfmons), refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about alarms, refer to the *Cisco Unified Serviceability Administration Guide*.

This section provides information to help you troubleshoot problems with Cisco Communications Manager Extension Mobility:

Related Topics

Troubleshooting Cisco Extension Mobility Error Messages, on page 104
Troubleshooting General Problems with Cisco Extension Mobility, on page 104

Troubleshooting General Problems with Cisco Extension Mobility

If any problems occur with Cisco Extension Mobility, start with these troubleshooting tips:

- Configure the Cisco Extension Mobility trace directory and enable debug tracing by performing the following procedures:
  - From Cisco Unified Serviceability, choose **Trace > Trace Configuration**
  - From the Servers drop-down list, choose a server.
  - From the drop-down menu of Configured Services, choose **Cisco Extension Mobility**.
- Make sure that you entered the correct URL for the Cisco Extension Mobility service. Remember that the URL is case sensitive.
- Check that you have thoroughly and correctly performed all the configuration procedures.
- If a problem occurs with authentication of a Cisco Extension Mobility user, go to the user pages and verify the PIN.

If you are still having problems, use the troubleshooting solutions in the following table.

Table 8: Troubleshooting Cisco Unified Communications Manager Extension Mobility

Problem Description	Recommended Action
After a user logs out and the phone reverts to the default device profile, the user finds that the phone services are no longer available.	**1.** Check the Enterprise Parameters to make sure that the Synchronization Between Auto Device Profile and Phone Configuration is set to **True**. **2.** Subscribe the phone to the Cisco Extension Mobility service.
After logging in, the user finds that the phone services are not available.	This problem occurs because the User Profile did not have any services that were associated with it when the profile was loaded on the phone. Perform the following steps: **1.** Change the User Profile to include the Cisco Extension Mobility service. **2.** Change the phone configuration where the user is logged in to include Cisco Extension Mobility. After the phone is updated, the user can access the phone services.
After performing a login or logout, the user finds that the phone resets instead of restarting.	Locale change may provide the basis for reset. If the User Locale that is associated with the login user or profile is not the same as the locale or device, after a successful login, the phone will perform a restart that is followed by a reset. This occurs because the phone configuration file is being rebuilt.

Troubleshooting Cisco Extension Mobility Error Messages

Use the information in the following table to troubleshoot the error codes and error messages that display on the phone when Cisco Extension Mobility is used.

Table 9: Troubleshooting Error Messages That Display on the Phone

Error Code	Message on Phone	Recommended Action
201	[201]-Authentication error	The user should check that the correct UserID and PIN were entered; the user should check with the system administrator that the UserID and PIN are correct.
22	[22]-Dev.logon disabled	Make sure that you have chosen "Enable Extension Mobility" check box on the Phone Configuration window. Refer to the Feature Configuration Guide for Cisco Unified Communications Manager.
205	[205]-User Profile Absent	Make sure that you have associated a Device Profile to the user Feature Configuration Guide for Cisco Unified Communications Manager.
208	[208]-EMService Conn. error	Verify that the Cisco Extension Mobility service is running by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.
25	[25]-User logged in elsewhe..	Check whether the user is logged in to another phone. If multiple logins need to be allowed, ensure the Multiple Login Behavior service parameter is set to Multiple Logins Allowed.
	Host not found	Check that the Cisco Tomcat service is running by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Network Services**.
	Http Error [503]	If you get this error when Services button is pressed, check that the Cisco Communications Manager Cisco IP Phone Services service is running by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Network Services**. If you get this error when you select Extension Mobility service, check that the Cisco Extension Mobility Application service is running by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Network Services**.
202	[202]-Blank userid or pin	Enter a valid userid and PIN.
26	[26]- Busy, please try again	Check whether the number of concurrent login/logout requests is greater than the Maximum Concurrent requests service parameter. If so, lower the number of concurrent requests. To verify the number of concurrent login/logout requests, use Unified Communications Manager Cisco Unified Real-Time Monitoring Tool to view the Requests In Progress counter in the Extension Mobility object.
6	[6]-Database Error	Check whether a large number of requests exists If large number of requests exists, the Requests In Progress counter in the Extension Mobility object counter specifies a high value. If the requests are rejected due to large number of concurrent requests, the Requests Throttled counter also specifies a high value. Collect detailed database logs.

Error Code	Message on Phone	Recommended Action
207	[207]-Device Name Empty	Check that the URL that is configured for Cisco Extension Mobility is correct.

Troubleshooting Cisco Unified Communications Manager Assistant

This section covers solutions for the most common issues that relate to Cisco Unified Communications Manager Assistant.

The following table describes troubleshooting tools for Unified CM Assistant and the client desktop.

Table 10: Cisco Unified Communications Manager Assistant Troubleshooting Tools and Client Desktop

Tool Description	Location
Cisco UnifiedCM Assistant server trace files	The log files reside on the server that runs the Cisco IP Manager Assistant service. You can download these files from the server by using one of the following methods: • Use the CLI command: **file get activelog tomcat/logs/ipma/log4j** • Use the trace collection features in the Unified CM Cisco Unified Real-Time Monitoring Tool (RTMT). Refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* for more information. You can enable debug tracing by choosing **Cisco Unified Serviceability** > **Trace** > **Configuration**.
Cisco IPMA client trace files	`$INSTALL_DIR\logs\ACLog*.txt` on the client desktop in the same location where the Unified CM Assistant assistant console resides. To enable debug tracing, go to the settings dialog box in the assistant console. In the advanced panel, check the Enable Trace check box. **Note** This enables only debug tracing. Error tracing always remains On.
Cisco IPMA client install trace files	`$INSTALL_DIR\InstallLog.txt` on the client desktop in the same location where the Unified CM Assistant assistant console resides.
Cisco IPMA Client AutoUpdater trace files	`$INSTALL_DIR\UpdatedLog.txt` on the client desktop in the same location where the Unified CM Assistant assistant console resides.
Install directory	By default—`C:\Program Files\Cisco\Unified Communications Manager Assistant Console\`

Related Topics

IPMAConsoleInstall.jsp Displays Error: HTTP Status 503-This Application is Not Currently Available, on page 107
IPMAConsoleInstall.jsp Displays Error: No Page Found Error, on page 107
Exception: java.lang.ClassNotFoundException: InstallerApplet.class, on page 108
Automatic Installation of MS Virtual Machine Is No Longer Provided..., on page 108
User Authentication Fails, on page 109
Assistant Console Displays Error: System Error - Contact System Administrator, on page 109
Assistant Console Displays Error: Cisco IP Manager Assistant Service Unreachable, on page 110
Calls Do Not Get Routed When Filtering Is On or..., on page 111
Cisco IP Manager Assistant Service Cannot Initialize, on page 112
Calling Party Gets a Reorder Tone, on page 113
Manager Is Logged Out While the Service Is Still Running..., on page 113
Manager Cannot Intercept Calls That Are Ringing on the Assistant..., on page 114
Not Able to Call the Manager Phone When Cisco IP..., on page 114

IPMAConsoleInstall.jsp Displays Error: HTTP Status 503-This Application is Not Currently Available

Symptom

`http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp` displays the following error message:

HTTP Status 503—This application is not currently available

Possible Cause

Cisco IP Manager Assistant service has not been activated or is not running.

Corrective Action

Make sure that the Cisco IP Manager Assistant service has been activated by checking the activation status of the service at **Cisco Unified Serviceability** > **Tools** > **Service Activation**.

If the Cisco IP Manager Assistant service has been activated, restart the Cisco Unified Communications Manager Assistant by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

IPMAConsoleInstall.jsp Displays Error: No Page Found Error

Symptom

`http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp` displays the following error message:

No Page Found Error

Possible Cause #1

Network problems.

Corrective Action #1

Ensure that the client has connectivity to the server. Ping the server name that is specified in the URL and verify that it is reachable.

Possible Cause #2

Misspelled URL.

Corrective Action #2

Because URLs are case sensitive, ensure that the URL matches exactly what is in the instructions.

Related Topics

Cisco Unified Communications Manager System Issues, on page 31

Exception: java.lang.ClassNotFoundException: InstallerApplet.class

Symptom

The assistant console fails to install from the web. The following message displays:

Exception: java.lang.ClassNotFoundException: InstallerApplet.class

Possible Cause

Using the Sun Java plug-in virtual machine instead of the Microsoft JVM with the standard Unified Communications Manager Assistant Console install causes failures.

Corrective Action

The administrator directs the user to the following URL, which is a JSP page that supports the Sun Java plug-in: `https://<servername>:8443/ma/Install/IPMAConsoleInstallJar.jsp`

Automatic Installation of MS Virtual Machine Is No Longer Provided for Download

Symptom

The Assistant Console fails to install from the web when you are trying to install on a computer that is running Microsoft Windows XP. A message displays that all the components for the program are not available. When the user chooses Download Now, the following message displays:

Automatic installation of MS Virtual Machine is no longer available for download

Possible Cause

Microsoft does not support Microsoft JVM in IE version 6 of Windows XP.

Note This error does not occur if you have the Microsoft JVM with XP Service Pack 1 installed on your system.

Corrective Action

Perform one of the following corrective actions:

- Install the Netscape browser (version 7.x) and use Netscape to install the assistant console.
- Install the Sun Java Virtual Machine plug-in for IE from the following URL:

  `http://java.sun.com/getjava/download.html`

  When the Sun Java plug-in completes installation, point the browser at the following URL:

  `https://<servername>:8443/ma/Install/IPMAInstallJar.jsp`
- Install the Microsoft Java Virtual Machine (JVM) with Windows XP Service Pack 1 before the assistant console installation.

User Authentication Fails

Symptom

User authentication fails when you sign in on the login window from the assistant console.

Possible Cause

The following probable causes can apply:

- Incorrect administration of the user in the database.
- Incorrect administration of the user as an assistant or a manager.

Corrective Action

Ensure that the user ID and the password are administered as a Unified Communications Manager user through Unified Communications Manager.

You must administer the user as an assistant or a manager by associating the Unified Communications Manager Assistant user information, which you access through **Unified Communications Manager Administration** > **User Management** > **End User**.

Assistant Console Displays Error: System Error - Contact System Administrator

Symptom

After launching the Assistant Console, the following message displays:

System Error - Contact System Administrator

Possible Cause #1

You may have upgraded the Unified Communications Manager from 4.x release to a 5.x release. The system cannot automatically upgrade the assistant console from 4.x release to 5.x release.

Corrective Action #1

Uninstall the console by choosing **Start > Programs > Unified Communications Manager Assistant > Uninstall Assistant Console** and reinstall the console from URL `https://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp`.

Possible Cause #2

The user did not get configured correctly in the database.

Corrective Action #2

Ensure that the user ID and the password are administered as a Unified Communications Manager user through Cisco Unified Communications Manager Administration.

You must administer the user as an assistant or a manager by associating the Cisco Unified Communications Manager Assistant user information, which you access through **Unified Communications Manager Assistant** > **User Management** > **End User**. For more information, see Feature Configuration Guide for Cisco Unified Communications Manager.

Possible Cause #3

When you deleted a manager from an assistant, Cisco Unified Communications Manager AdministrationCisco Unified Communications Manager Administration left a blank line for the assistant.

Corrective Action #3

From the Assistant Configuration window, reassign the proxy lines. For more information, see Feature Configuration Guide for Cisco Unified Communications Manager.

Assistant Console Displays Error: Cisco IP Manager Assistant Service Unreachable

Symptom

After launching the assistant console, the following message displays:

Cisco IPMA Service Unreachable

Probable Cause #1

Cisco IP Manager Assistant service may have stopped.

Corrective Action #1

Restart the Cisco Unified Communications Manager Assistant by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Probable Cause #2

The server address for the Primary and Secondary Cisco Unified Communications Manager Assistant servers may be configured as DNS names, but the DNS names are not configured in the DNS server.

Corrective Action #2

Use the following procedure to replace the DNS name.

Procedure

1. Choose **Unified Communications Manager Administration** > **System** > **Server**.
2. Replace the DNS name of the server with the corresponding IP address.
3. Restart the Cisco Unified Communications Manager Assistant by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Probable Cause #3

The *Cisco CTI Manager* service may have stopped.

Corrective Action #3

Restart the *Cisco CTI Manager* and *Cisco IP Manager Assistant* services by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Probable Cause #4

The Cisco Unified Communications Manager Assistant service might have been configured to open a CTI connection in secure mode, but the security configuration may not be complete.

If this occurs, the following message displays in the alarm viewer or in the Cisco Unified Communications Manager Assistant service logs:

IPMA Service cannot initialize - Could not get Provider.

Corrective Action #4

Check the security configuration in the service parameters of *Cisco IP Manager Assistant* service. For more information, see Feature Configuration Guide for Cisco Unified Communications Manager.

Restart the Cisco Unified Communications Manager Assistant by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Calls Do Not Get Routed When Filtering Is On or Off

Symptom

Calls do not get routed properly.

Possible Cause #1

Cisco CTI Manager service may have stopped.

Corrective Action #1

Restart the *Cisco CTI Manager* and *Cisco IP Manager Assistant* services by choosing **Cisco Unified Serviceability > Tools > Control Center—Feature Services**.

Possible Cause #2

The Unified Communications Manager route point did not get configured properly.

Corrective Action #2

Use wild cards to match the directory number of the Unified Communications Manager CTI route point and the primary directory numbers of all managers that are configured for Unified Communications Manager.

Possible Cause #3

The status window on the manager phone displays the message, Filtering Down. This can indicate that Unified Communications Manager Assistant CTI route point may be deleted or may not be in service.

Corrective Action #3

Use the following procedure to configure the CTI route point and restart the *Cisco IP Manager Assistant* service.

Procedure

1. From Unified Communications Manager, choose **Device** > **CTI Route Point**.
2. Find the route point, or add a new route point. See System Configuration Guide for Cisco Unified Communications Manager for configuration details.
3. Restart the Cisco IP Manager Assistant services by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Cisco IP Manager Assistant Service Cannot Initialize

Symptom

The *Cisco IP Manager Assistant* service cannot open a connection to CTI Manager, and the following message displays:

IPMA Service cannot initialize - Could not get Provider.

Possible Cause

The *Cisco IP Manager Assistant* service cannot open a connection to CTIManager. You can see the message in the alarm viewer or in the Cisco Unified Communications Manager Assistant service logs.

Corrective Action

Restart the Cisco CTI Manager and *Cisco IP Manager Assistant* services by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Calling Party Gets a Reorder Tone

Symptom

Calling party gets a reorder tone or a message: “This call cannot be completed as dialed.”

Possible Cause

You may not have configured the calling search space of the calling line correctly.

Corrective Action

Check the calling search space of the line. For the configuration details, see the System Configuration Guide for Cisco Unified Communications Manager.

You can also use the Cisco *Dialed Number Analyzer* service to check any flaws in the calling search space. For more details, see *Cisco Unified Communications Manager Dialed Number Analyzer Guide* for more details.

Manager Is Logged Out While the Service Is Still Running

Symptom

Although the manager is logged out of Unified Communications Manager Assistant, the service still runs. The display on the manager IP phone disappears. Calls do not get routed, although filtering is on. To verify that the manager is logged out, view the application log by using the Cisco Unified Real-Time Monitoring Tool. Look for a warning from the Cisco Java Applications that indicates that the Cisco IP Manager Assistant service logged out.

Possible Cause

The manager pressed the softkeys more than four times per second (maximum limit allowed).

Corrective Action

The Unified Communications Manager administrator must update the manager configuration. Perform the following procedure to correct the problem.

Procedure Action

1. From Unified Communications Manager Administration, choose **User Management** > **End User**.

   The Find and List Users window displays.
2. Enter the manager name in the search field and click the **Find**.
3. Choose the manager from the results list that you want to update.

   The End User Configuration window displays.
4. From the Related Links drop-down list box, choose **Cisco IPMA Manager** and click **Go**.
5. Make the necessary changes to the manager configuration and click **Update**.

Manager Cannot Intercept Calls That Are Ringing on the Assistant Proxy Line

Symptom

The manager cannot intercept the calls that are ringing on the assistant proxy line.

Possible Cause

The calling search space of the proxy line did not get configured properly.

Corrective Action

Check the calling search space of the proxy line for the assistant phone. Perform the following procedure to correct the problem.

Procedure Action

1. From Unified Communications Manager Administration , choose **Device > Phone**.

   The Find and List Phones search window displays.

2. Click the assistant phone.

   The Phone Configuration window displays.

3. Verify the calling search space configuration for the phone and for the directory number (line) and update as appropriate.

Not Able to Call the Manager Phone When Cisco IP Manager Assistant Service is Down

Symptom

Calls do not get routed properly to managers when Cisco IP Manager Assistant service goes down.

Possible Cause

The Cisco Unified Communications Manager Assistant CTI route point did not get enabled for Call Forward No Answer.

Corrective Action

Perform the following procedure to properly configure the Cisco Unified Communications Manager Assistant route point.

Procedure Action

1. From Cisco Unified Communications Manager Administration, choose **Device** > **CTI Route Point**.

   The Find and List CTI Route Point search window displays.

2. Click the **Find** button.

A list of configured CTI Route Points display.

3. Choose the Cisco Unified Communications Manager Assistant CTI route point that you want to update.
4. In the CTI Route Point Configuration window, click the line to update from the Directory Numbers box.

   The Directory Number Configuration window displays.
5. In the Call Forward and Pickup Settings section, check the Forward No Answer Internal and/or the Forward No Answer External check box and enter the CTI route point DN in the Coverage/Destination field (for example, CFNA as 1xxx for the route point DN 1xxx).
6. In the Calling Search Space drop-down list, choose CSS-M-E (or appropriate calling search space).
7. Click the **Update**.

Troubleshooting Cisco Unified Mobility

This section provides information to help you troubleshoot problems with Cisco Unified Mobility.

Related Topics

Cisco Unified Mobility User Hangs Up Mobile Phone But Cannot..., on page 115
Dial-via-Office-Related SIP Error Codes, on page 116

Cisco Unified Mobility User Hangs Up Mobile Phone But Cannot Resume Call on Desktop Phone

Symptom

When a remote destination (mobile phone) is not a smart phone and a call to this mobile phone is anchored through Unified Communications Manager, the user can hang up the mobile phone and expect to see a **Resume** softkey on the user desktop phone to resume the call. The user cannot resume this call on the user desktop phone.

Possible Cause

If the calling party receives busy/reorder/disconnect tone when the mobile phone hangs up, the mobile phone provider probably did not disconnect the media. Unified Communications Manager cannot recognize this circumstance, because no disconnect signals came from the provider. To verify whether this is the case, let the calling party wait 45 seconds, when service provider will time out and send disconnect signals, upon which Unified Communications Manager can provide a **Resume** softkey to resume the call.

Recommended Action

Perform the following actions:

- Add the following command to the gateway:

  voice call disc-pi-off
- For the Cisco CallManager service, set the Retain Media on Disconnect with PI for Active Call service parameter to False.

Dial-via-Office-Related SIP Error Codes

Symptom

A Cisco Unified Mobility Dial-via-Office (DVO) call does not succeed.

Possible Cause

Unified Communications Manager provides specific SIP error codes when a dial-via-office call does not succeed. The following table provides the SIP error codes for unsuccessful dial-via-office calls.

Call Scenario	SIP Error Code
Target number is not routable.	404 Not Found
Target is busy.	486 Busy Here
Cisco Unified Mobile Communicator hangs up before target answers.	487 Request Terminated
Cisco Unified Mobile Communicator sends SIP CANCEL.	487 Request Terminated
Cisco Unified Mobile Communicator tries to make a call without successful registration.	503 Service Unavailable
Cisco Unified Mobile Communicator tries to make a call when there are already two outstanding calls on the enterprise line.	486 Busy Here
Cisco Unified Mobile Communicator tries to make a DVO-F call when there is an outstanding pending DVO-F call (awaiting PSTN call).	487 Request Terminated (on the first call)

Troubleshooting Cisco Web Dialer

This section covers error messages for the most common issues that relate to Cisco Web Dialer.

Related Topics

Authentication Error, on page 117
Cisco CTIManager Down, on page 118
Destination Not Reachable, on page 119
Directory Service Down, on page 117
Failed to Open Device/Line, on page 119
Service Temporarily Unavailable, on page 117
Session Expired, Please Login Again, on page 118
User Not Logged in on Any Device, on page 118

Authentication Error

Symptom

Cisco Web Dialer displays the following message:

Authentication failed, please try again.

Probable Cause

User entered wrong userID or password

Corrective Action

Check your userID and password. You must log in by using your Unified Communications Manager userID and password.

Service Temporarily Unavailable

Symptom

Cisco Web Dialer displays the following message:

Service temporarily unavailable, please try again later.

Possible Cause

The Cisco CallManager service got overloaded because it has reached its throttling limit of three concurrent CTI sessions.

Corrective Action

After a short time, retry your connection.

Directory Service Down

Symptom

Cisco Web Dialer displays the following message:

Service temporarily unavailable, please try again later: Directory service down.

Possible Cause

The Cisco Communications Manager directory service may be down.

Corrective Action

After a short time, retry your connection.

Cisco CTIManager Down

Symptom

Cisco Web Dialer displays the following message:

Service temporarily unavailable, please try again later: Cisco CTIManager down.

Possible Cause

Cisco CTIManager service that is configured for Cisco Web Dialer went down.

Corrective Action

After a short time, retry your connection.

Session Expired, Please Login Again

Symptom

Cisco Web Dialer displays the following message:

Session expired, please login again.

Possible Cause

A Cisco Web Dialer session expires

- After the Web Dialer servlet gets configured or
- If the Cisco Tomcat Service is restarted.

Corrective Action

Log in by using your Unified Communications Manager userID and password.

User Not Logged in on Any Device

Symptom

Cisco Web Dialer displays the following message:

User not logged in on any device.

Possible Cause

The user chooses to use Cisco Extension Mobility from the Cisco Web Dialer preference window but does not get logged in to any IP phone.

Corrective Action

- Log in to a phone before using Cisco Web Dialer.

- Choose a device from the Cisco Web Dialer preference list in the dialog box instead of choosing the option **Use Extension Mobility**.

Failed to Open Device/Line

Symptom

After a user attempts to make a call, Cisco Web Dialer displays the following message:

User not logged in on any device.

Possible Cause

- The user chose a Cisco Unified IP Phone that is not registered with Unified Communications Manager. For example, the user chooses a Cisco IP SoftPhone as the preferred device before starting the application.
- The user who has a new phone chooses an old phone that is no longer in service.

Corrective Action

Choose a phone that is in service and is registered with Unified Communications Manager.

Destination Not Reachable

Symptom

Cisco Web Dialer displays the following message on the End Call window:

Destination not reachable.

Possible Cause

- User dialed the wrong number.
- The correct dial rules did not get applied. For example, the user dials 5550100 instead of 95550100.

Corrective Action

Check the dial rules.

Troubleshooting Directed Call Park

The following table provides troubleshooting recovery tips for common directed call park problems.

Table 11: Troubleshooting Tips for Directed Call Park

Problem Description	Recommended Action
User cannot park calls. After the Transfer softkey (or Transfer button if available) is pressed and the directed call park number is dialed, the call does not get parked.	Ensure that the partition that is assigned to the call park number matches the partition that is assigned to the phone directory number. See the . Ensure that the partition and calling search space are configured correctly for the device. See the .
User cannot park calls. After pressing the Transfer softkey (or Transfer button if available) and dialing the directed call park number, the user receives a busy tone, and the IP phone displays the message, Park Slot Unavailable.	Ensure that the dialed directed call park number is not already occupied by a parked call or park the call on a different directed call park number.
User cannot park calls. After pressing the Transfer softkey (or Transfer button if available) and dialing the directed call park number, the user receives a reorder tone or announcement.	Ensure that the dialed number is configured as a directed call park number. See the Feature Configuration Guide for Cisco Unified Communications Manager.
Parked calls revert too quickly.	Set the Call Park Reversion Timer to a longer duration. See the Feature Configuration Guide for Cisco Unified Communications Manager
User cannot park calls. The user receives a reorder tone after the reversion timer expires.	Ensure that the user presses the Transfer softkey (or Transfer button if available) before dialing the directed call park number, then presses the Transfer softkey (or Transfer button) again or goes on hook after dialing the directed call park number. Because directed call park is a transfer function, the directed call park number cannot be dialed alone. See the Feature Configuration Guide for Cisco Unified Communications Manager **Note** You can complete the transfer only by going on hook rather than pressing the Transfer softkey (or Transfer button) a second time if the Transfer On-hook Enabled service parameter is set to True. See the Feature Configuration Guide for Cisco Unified Communications Manager.
User cannot retrieve parked calls. After dialing the directed call park number to retrieve a parked call, the user receives a busy tone, and the IP phone displays the message, Park Slot Unavailable.	Ensure that the user dials the retrieval prefix followed by the directed call park number. See the Feature Configuration Guide for Cisco Unified Communications Manager.
Parked calls do not revert to the number that parked the call.	Check the configuration of the directed call park number to ensure that it is configured to revert to the number that parked the call rather than to a different directory number. See the Feature Configuration Guide for Cisco Unified Communications Manager.
When an attempt is made to delete a directed call park number or range, a message displays that indicates that the number or range cannot be deleted because it is in use.	You cannot delete a directed call park number that a device is configured to monitor (by using the BLF button). To determine which devices are using the number, click the Dependency Records link on the Directed Call Park Configuration window.

Problem Description	Recommended Action
After configuring a range of directed call park numbers, user cannot park a call at a number within the range.	Review the syntax for entering a range of directed call park numbers. If incorrect syntax is used, the system may appear to configure the range when it actually does not. See the Feature Configuration Guide for Cisco Unified Communications Manager.

Troubleshooting External Call Control

This section describes how to handle some common external call control issues.

Unified Communications Manager cannot connect to the adjunct route server.

- The URI in the External Call Control Profile window in Cisco Unified Communications Manager Administration is not correct. (**Call Routing** > **External Call Control**)
  - Verify the URI for the adjunct route server. Ensure that the URI uses the following formula:

    ```
    https://<hostnameor IPv4 address of route server>:<port that is
    configured on route server>/path from route server configuration
    ```

  - If the adjunct route server uses https, verify that you imported and exported the required certificates, as described in the "External Call Control" chapter in the System Configuration Guide for Cisco Unified Communications Manager.
  - If the adjunct route server uses https, verify that hostname that you enter for the URI for the Primary Web Service and Secondary Web Services fields in the External Call Control Profile window in Cisco Unified Communications Manager Administration matches the hostname that is in the adjunct route server certificate.
- Network connectivity dropped between Unified Communications Manager and the adjunct route server. Because the Connection Loss and PDP Out Of Service counters are incrementing counters, they indicate that at one time good connections were made to the adjunct route server. Therefore, an event in the network caused the problem, or an event occurred on the adjunct route server.
  - Verify that the adjunct route server is running and that network connectivity is good.
- Unified Communications Manager routing query to the adjunct route server times out because of slow response from the adjunct route server. The adjunct route server may be overloaded because of processing service requests, or network instability occurred.
  - Increase the value for the Routing Request Timer in the external call control profile, or increase the value for the External Call Control Routing Request Timer service parameter.
  - Increase the value for the External Call Control Maximum Connection Count To PDP service parameter.
  - Add a secondary web service (redundant adjunct route server) in the external call control profile and enable load balancing in the profile.
- The Unified Communications Manager routing request failed when Unified Communications Manager failed to parse the routing directive from the adjunct route server.

- Verify that the XACML or CIXML is correctly formatted. Both the XACML request and response display in the Cisco CallManager SDI trace. The routing response code for each routing request exists in the trace. A value of 0 means the request was received and parsed correctly.

Call failed due to exceed maximum diversion hops or maximum diversion hops to the same translation pattern.

- A caller receives reorder tone.
- Check the Cisco CallManager SDI trace. For example, if the External Call Control Diversion Maximum Hop Count service parameter is 12. the Cisco CallManager SDI trace shows:

```
PER_RoutingCallInfo::isCallDiversionMaximumHopCountExceeded:
callDiversionHopCount(12) >= CallDiversionMaximumHopCountLimit(12)
```

- For example, if the Maximum External Call Control Diversion Hops to Pattern or DN service parameter is 12, the Cisco CallManager SDI trace shows:

```
PER_RoutingCallInfo::isCallDiversionMaximumHopToSamePatternCountExceeded:
CallDiversionHopToSamePatternCount(12) >=
CallDiversionMaximumHopToSamePatternCountLimit(12)
```

- Verify the service parameter configuration, and change, if necessary.
- Verify the obligation configuration on the adjunct route server for call redirection. For example, A calls B; the route for B indicates to divert A to C; the route for C says indicates to divert A to D. D has CFA enabled to E. The route for E says to divert to A to F, and so on.

Unified Communications Manager cannot parse the call routing directives, mandatory parameters, or XACML from the adjunct route server.

- RTMT show the error alarm, ErrorParsingDirectiveFromPDP. This alarm contains one of following reasons.
  - Error parsing the route decision from adjunct route server.
  - The route decision from the adjunct route server is indeterminate.
  - The route decision from adjunct route server is not applicable.

Tip For the preceding bullets, check the adjunct route server route rule and configuration. Unified Communications Manager routes the call based on the failure treatment.

- An adjunct route server diverts a call without a destination in the obligation.

Tip Check the obligation configuration on the adjunct route server. The obligation should have a destination for the call routing directive = divert.

- Call was denied. The adjunct route server denies a call, but the CIXML response contains an obligation other than reject.

Tip On the adjunct route server, check that the obligation for the call routing directive = reject. The preceding bullet supports the case where the route is deny, but the obligation is not reject.

Unified Communications Manager failed to parse one or multiple optional attributes in a call routing response from the adjunct route server.

- RTMT displays the warning alarm, ErrorParsingResponseFromPDP. This alarm contains one or combination of following reasons depending on whether there is one or multiple errors.
  - Request Processing Error—Check adjunct route server trace for error.
  - XACML Syntax Error—Check the route configuration on the adjunct route server.
  - CIXML Missing Optional Attribute—Check obligation configuration on the adjunct route server.
  - CIXML Syntax Error—Check obligation configuration on the adjunct route server.
  - Invalid announcement Id—Check obligation configuration on the adjunct route server.

Unified Communications Manager cannot fulfill a call routing directive returned by the adjunct route server because of Unified Communications Manager feature interaction and/or Unified Communications Manager configuration.

- Unified Communications Manager cannot fulfill a call routing directive. Unified Communications Manager cannot route a call to a destination. A caller receives reorder tone. A caller does not receive announcement. Unified Communications Manager generates the FailedToFulfillDirectiveFromPDP alarm.
- RTMT shows the warning alarm, FailedToFulfillDirectiveFromPDP. This alarm contains one of following reasons.
  - Insert of the announcement failed.—Check whether the Cisco IP Voice Media Streaming App service is running in Cisco Unified Serviceability. If it is running, check that the Annunciator service parameter for the Cisco IP Voice Media Streaming App service is set to True. Furthermore, there could be codec mismatch. The annunciator supports G.711, G.729, and Cisco Wideband codec, which the caller device may not support.
  - Announcement can't be played because no early media capability.—The caller device does not supports the early media capability. Some devices that support the early media capability are SIP trunk and H323 trunk.
  - Redirect Call Error with Error Code.—Check the Diversion Rerouting Calling Search Space configured in the external call control profile to determine whether it includes the partition of a redirected destination/device.
  - Extend Call Error with Error Code.—Perhaps a destination is busy or unregistered, or the destination pattern is a translation pattern that is not associated with a device.

Unified Communications Manager Administration reports an error processing an uploaded custom announcement.

- Verify that the custom announcement.wav file is in proper format; that is, Windows PCM, 16-bit, (16000, 32000, 48000, or 48100) samples per second, mono or stereo.
- In RTMT, collect the Cisco Audio Translator traces for analysis of the error.

No announcement gets played.

The Cisco IP Voice Media Streaming App service issues the following alarms:

- kANNAudioUndefinedAnnID—The announcement uses an undefined custom announcement identifier or locale identifier. The alarm contain the numeric identifiers.
- kANNAudioFileMissing— Custom and/or Cisco-provided announcement.wav file is not found. The alarm contains file name, Announcement ID, user locale, and network locale.
- Verify ANN device is registered to the Unified Communications Manager.
- If media resource group is being used, verify that the ANN device is in media resource group.
- Verify that the announcement ID is correct.
- Verify that the locale is installed if you are not using English, United States locale.

Troubleshooting Hotline

The following table provides troubleshooting information for cases where hotline calls do not dial correctly.

Table 12: Troubleshooting Hotline—Calls Do Not Dial Correctly

Problem	Solution
Dial tone	Check PLAR configuration.
Reorder tone or VCA (intracluster call)	• Check PLAR configuration. • Verify that the phones on both ends are configured as hotline phones.
Reorder tone or VCA (intercluster or TDM call)	• Check PLAR configuration. • Verify that the phones on both ends are configured as hotline phones. • Verify that route class signalling is enabled on trunks. • Check the configuration of route class translations on CAS gateways.

The following table provides troubleshooting information for cases where call screening based on caller ID does not work.

Table 13: Troubleshooting Hotline—Call Screening Based on Caller ID Problems

Problem	Solution
Call not allowed	• Check Caller ID. • Add pattern to screen CSS.
Call allowed	Remove pattern from screen CSS.

Troubleshooting Immediate Divert

This section covers solutions for the most common issues that relate to the Immediate Divert feature.

Related Topics

Busy, on page 126
Key is not active, on page 125
Temporary Failure, on page 125

Key Is Not Active

Symptom

This message displays on the phone when the user presses iDivert.

Possible Cause

The voice-messaging profile of the user who pressed iDivert does not have a voice-messaging pilot.

Corrective Action

Configure a voice-messaging pilot in the user voice-messaging profile.

Temporary Failure

Symptom

This message displays on the phone when the user presses iDivert.

Possible Cause

The voice-messaging system does not work, or a network problem exists.

Corrective Action

Troubleshoot your voice-messaging system. See troubleshooting or voice-messaging documentation.

Busy

Symptom

This message displays on the phone when the user presses iDivert.

Possible Cause

Message means that the voice-messaging system is busy.

Corrective Action

Configure more voice-messaging ports or try again.

Troubleshooting Intercom

This section covers the solutions for the most common issues that relate to Intercom.

Related Topics

Getting Busy Tone When Dialing Out of Intercom Line, on page 126
Intercom Calls Do Not Go to Connected State When Going..., on page 126
Troubleshooting SCCP, on page 127
Troubleshooting SIP, on page 128
Cisco Extension Mobility User Is Logged In But Intercom Line..., on page 128

Getting Busy Tone When Dialing Out of Intercom Line

Symptom

Phone plays busy tone when user is dialing out of intercom line.

Possible Cause

DN is not in the same intercom partition as the calling number.

Recommended Action

1. Ensure that the DN is in the same intercom partition as the calling number.
2. If it is, ensure that the dialed out DN is configured on another phone and that phone is registered with same Unified Communications Manager cluster.

Intercom Calls Do Not Go to Connected State When Going Off Hook by Using Speaker, Handset, or Headset

Symptom

User cannot go into talkback mode for intercom calls by using headset, handset, or speaker.

Possible Cause

This situation exists by design. The only way to go into the connected state for intercom calls is by pressing the corresponding line button.

Recommended Action

User can end call by using speaker, handset, or headset.

Troubleshooting SCCP

This section provides troubleshooting tips for phones that are running SCCP.

Related Topics

Intercom Lines Not Showing Up on Phone When Button Template..., on page 127
Intercom Lines Not Showing Up When Phone Falls Back to..., on page 127

Intercom Lines Not Showing Up on Phone When Button Template Has Them

Symptom

Intercom lines do not display on the phone.

Possible Cause

The phone version may be earlier than 8.3(1), or the button template may not be assigned to the phone.

Procedure

1. Check the phone version. Ensure that it is 8.3(1) or above.
2. Determine whether the button template is assigned to the phone.
3. Capture the sniffer trace between Unified Communications Manager and the phone. In the button template response, see whether intercom lines get sent to the phone (button definition = Ox17).

Intercom Lines Not Showing Up When Phone Falls Back to SRST

Symptom

The phone, which was configured with Unified Communications Manager Release 6.0(x) or later, includes two intercom lines. Unified Communications Manager stops and falls back to SRST. The intercom lines do not display.

Possible Cause

The SCCP version of SRST does not support SCCP version 12.

Recommended Action

1. Check the SCCP version of SRST. If SRST supports SCCP version 12, it will support intercom lines.

2. If SRST supports SCCP version 12, capture a sniffer trace and ensure that the button template that the phone sent includes intercom lines.

Troubleshooting SIP

This section provides information to help you determine issues on phones that are running SIP.

Related Topics

Configuration of Phones That Are Running SIP, on page 128
Debugging Phones That Are Running SIP, on page 128

Debugging Phones That Are Running SIP

Use this debug command, **Debug sip-messages sip-task gsmfsmIsm sip-adapter**.

Configuration of Phones That Are Running SIP

Show config - The command on the phone displays if intercom lines are configured as regular lines with featureid-->23.

Cisco Extension Mobility User Is Logged In But Intercom Line Does Not Display

Symptom

The *Cisco Extension Mobility* user is logged into a phone, but the user intercom line does not display.

Possible Cause

Default Activated Device is configured incorrectly.

Recommended Action

1. Check that the Default Activated Device is configured on the intercom directory number.
2. Check that the Default Activated Device matches the device to which the used in logged in.

Where to Find More Information

- “Intercom” chapter, Feature Configuration Guide for Cisco Unified Communications Manager.

Troubleshooting IPv6

This section describes corrective actions for issues that are related to IPv6.

Related Topics

Calls Between Devices Fail, on page 130
Calls Over SIP Trunks Fail, on page 129
Music On Hold Does Not Play on Phone, on page 130

Phones Do Not Register with Cisco Unified Communications Manager, on page 129

Phones Do Not Register with Cisco Unified Communications Manager

Symptom

Cisco Unified IP Phones with an IP Addressing Mode of IPv6 Only do not register with Unified Communications Manager.

Corrective Action

- Via the CLI, verify that you enabled IPv6 on the Unified Communications Manager server.
- In the Enterprise Parameter Configuration window, verify that the Enable IPV6 enterprise parameter is set to True.
- In the Server Configuration window, verify that you configured either the host name or the IPv6 address for the Unified Communications Manager server in the Ipv6 Name field. If you configured a host name, verify that you configured DNS to resolve the host name to an IPv6 address.
- Verify that the Unified Communications Manager server has one non link-local IPv6 address only.
- If the phone gets an IPv6 address via stateless autoconfiguration, verify that you configured the Allow Auto-Configuration for Phone setting as On.
- Verify that the Cisco CallManager and Cisco TFTP services are running.

Calls Over SIP Trunks Fail

Symptom

Incoming calls fail if they come over a SIP trunk that has an IP Addressing Mode of IPv6 Only.

Corrective Action

- Via the CLI, verify that you enabled IPv6 on the Unified Communications Manager server.
- In the Enterprise Parameter Configuration window, verify that the Enable IPV6 enterprise parameter is set to True.
- Verify that the INVITE does not contain IPv4 signaling.

Symptom

Outgoing calls fail if they come over a SIP trunk that has an IP Addressing Mode of IPv6 Only.

Corrective Action

- Via the CLI, verify that you enabled IPv6 for the operating system on the Unified Communications Manager server.
- In the Enterprise Parameter Configuration window, verify that the Enable IPV6 enterprise parameter is set to True.

- In the Trunk Configuration window, verify that you configured an IPv6 destination address for the SIP trunk.

Calls Between Devices Fail

Symptom

Calls between two devices fail.

Corrective Action

- In the device configuration window, verify the IP addressing mode of the devices.
- If one device has an IP Addressing Mode of IPv4 Only and the other device has an IP Addressing Mode of IPv6 Only, ensure that you have an MTP configured that supports both the IPv4 and IPv6 stacks.

Music On Hold Does Not Play on Phone

Symptom

Phone user cannot hear music on hold.

Corrective Action

- Verify the IP addressing mode of the device where music on hold is played. If the IP addressing mode for the device is IPv6 Only and if music on hold is configured for unicast music on hold, ensure that you have an MTP configured that supports both the IPv4 and IPv6 stacks.
- If you configured multicast music on hold, be aware that phones that have an IP addressing mode of IPv6 Only cannot play music on hold.

Troubleshooting Logical Partitioning

This section describes corrective actions for issues that are related to logical partitioning.

Related Topics

Logical Partitioning Does Not Function As Expected, on page 130
Logical Partitioning Policies Require Adjustment, on page 131

Logical Partitioning Does Not Function As Expected

Symptom

Logical partitioning does not function as expected.

Corrective Action

Perform the following actions to correct the problem:

- Check whether the Enable Logical Partitioning enterprise parameter is set to **True**.
- Check that the device is associated with a valid geolocation at the device or device pool level.
- Check that the device is associated with a valid geolocation filter that comprises a selection of some of the geolocation fields at the device or device pool level.
- If the Logical Partitioning Default Policy enterprise parameter specifies **DENY**, check whether ALLOW logical partitioning policies between GeolocationPolicy of a gateway and GeolocationPolicy of a VoIP site are configured.
- Make sure that the case is correct for the fields of the logical partitioning GeolocationPolicy records and matches the case that is configured for geolocation records.
  - **Example:** The following geolocations exist: US:NC:RTP:BLD1 and US:TX:RCDN:bld1.

    When the GeolocationPolicy records get configured from logical partitioning policy records, you can configure the following policy: Border:US:NC:RTP:bld1 to Interior:US:NC:RTP:bld1.

    In this case, the incorrect value was chosen from the drop-down list box for the LOC field in the Location Partitioning Policy Configuration window, which displays both BLD1 and bld1.

    Therefore, the administrator must make sure to choose entries, so the case of the geolocation entry matches the case of the value that is used in GeolocationPolicy.
- No logical partitioning policy check takes place for VoIP-to-VoIP-device calls or features with only VoIP participants.
- Unified Communications Manager Administration allows configuration of policies between Interior:geolocpolicyX and Interior:geolocpolicyY, but such configuration does not get used during logical partitioning checks.

Logical Partitioning Policies Require Adjustment

Symptom

The fields in the logical partitioning policies are not configured correctly.

Corrective Action

Because the hierarchy of geolocation fields is significant, ensure that the hierarchical order of all fields is correct, and ensure that all fields are present. Hierarchical order means that Country entries precede A1 entries, which precede A2 entries, and so on.

Ensure that all fields are present in the logical partitioning policies and all fields are specified in the correct hierarchical order.

See the examples that follows.

Example of Logical Partitioning Policies That Match

In the following geolocation information, search for policy between Border:IN:KA and Interior:IN:KA.

The following possible policies match in order, where ***IN*** represents a Country field entry and KA represents an A1 field entry:

GeolocationPolicyA	GeolocationPolicyB	Policy
Border:IN:KA	Interior:IN:KA	Allow/Deny
Border:IN:KA	Interior:IN	Allow/Deny
Border:IN:KA	Interior	Allow/Deny
Border:IN	Interior:IN:KA	Allow/Deny
Border:IN	Interior:IN	Allow/Deny
Border:IN	Interior	Allow/Deny
Border	Interior:IN:KA	Allow/Deny
Border	Interior:IN	Allow/Deny
Border	Interior	Allow/Deny

Example of Logical Partitioning Policies That Do Not Match

In contrast, if the field of a geolocation is missing in a logical partitioning policy, the necessary match does not occur. The following logical partitioning policies do not include the Country field entry, which specifies ***IN***:

Border:KA
Interior:KA
Border:BLR
Interior:BLR
Border:KA:BLR
Interior:KA:BLR

Note Country=IN is missing.

Troubleshooting SIP with DNS Caching Enabled

Logging

Symptom

Set debug level for logging.

Recommended Action

Set network name-service debug-level 3(default 0)

- level 0 - no logging
- level 1 – errors, some cache removals
- level 2 – cache population
- level 3 and greater – entries considered for cache hits, pruning cache

Log file

Log file: activelog syslog/nscd.log

Consider the following example for Sample log file content:

Wed Dec 17 18:26:01 2014 - 21908: Have not found "clock.cisco.com" in hosts cache!

Wed Dec 17 18:26:01 2014 - 21908: add new entry "clock.cisco.com" of type GETHOSTBYNAME for hosts to cache (first)

Wed Dec 17 18:26:01 2014 - 21908: handle_request: request received (Version = 2) from PID 22151

Packet Capture

utils network capture port 53

Example:

admin: utils network capture port 53

Executing command with options:

```
size=128               count=1000              interface=eth0
 src=                   dest=                   port=53
 ip=  17:54:55.397539 IP b7k-vma150.cisco.com.45921 > dns-sj.cisco.com.domain: 38531+ A?
b7k-vma154.cisco.com.(38)
17:54:55.398952 IP b7k-vma150.cisco.com.44296 > dns-sj.cisco.com.domain: 63056+ PTR?
183.168.70.171.in-addr.arpa.(45)
17:54:55.430709 IP dns-sj.cisco.com.domain > b7k-vma150.cisco.com.45921: 38531* 1/3/6 A
10.94.12.154.(240)
```

```
17:54:55.431802 IP b7k-vma150.cisco.com.47404 > dns-sj.cisco.com.domain: 40244+ PTR?
154.12.94.10.in-addr.arpa.(43)
17:54:55.432016 IP dns-sj.cisco.com.domain > b7k-vma150.cisco.com.44296: 63056* 1/3/6 PTR
dns-sj.cisco.com.(261)
17:54:55.465242 IP dns-sj.cisco.com.domain > b7k-vma150.cisco.com.47404: 40244* 1/3/6 PTR
b7k-vma154.cisco.com.(263)
```

A/AAAA record caching is not working

Symptom

A/AAAA record caching is not working. An A/AAAA record query is sent every time SIP call needs host name resolution.

Corrective Action

Check the status of Name Service Cache service. The status should be“Started” as given below:

```
admin:utils service list
Requesting service status, please wait…
System SSH [STARTED]
Cluster Manager [STARTED]
Password Reset [STOPPED] Service Activated
Name Service Cache [STARTED]…
```

If the Name Service Cache service status is not STARTED, use the following CLI command to activate :

admin:utils service activateName Service Cache

admin:utils service start Name Service Cache

If the Name Service Cache service status is already STARTED, use the following CLI command to restart:

admin:utils service restart Name Service Cache

Set debug level to 3 or higher. Ping a valid host name. Check the nscd.log and verify that the A/AAAA record is being added to the cache or the system is utilizing an existing cache entry.

Events appear in system log (/var/log/active/syslog/messages).

Dec 17 10:41:31 localhost user 6 ilog_impl: Received request for platform-event (platform-system-startup)

Dec 17 10:41:31 localhost user 6 ilog_impl: emitting platform-event (platform-system-startup)

Dec 17 10:41:31 localhost user 6 ilog_impl: emitted platform-event (platform-system-startup)

Note If caching works for "ping", ensure that the caching works for the Unified Communications Manager Service (such as Cisco CallManager Service). There can be a delay for the application to detect and interact with nscd.

Hostname resolution returning wrong IP address

Symptom

Hostname resolution returns a wrong IP address.

Possible Cause

The cache is obsolete. This is usually due to A/AAAA record changes in DNS server.

Corrective Action

- Flush the current cache using the following CLI command:

admin:utils network name-service hosts cache invalidate

- If problem persists, restart nscd using the following CLI command:

admin:utils service restart Name Service Cache

- If problem still persists, disable nscd using the following CLI command:

admin: utils service stop Name Service Cache

- If problem still persists check the A/AAAA record configuration in the DNS server.

Cannot find log

Symptom

Cannot find log /var/log/active/syslog/nscd.log

Corrective Action

Check that the debug level is above 0 (default is 0). After updating debug level, restart nscd using the following CLI command:

admin:utils service restart Name Service Cache

Set nscd attributes through CLI

Symptom

I set nscd attributes via CLI, but the new attribute values are not taking effect.

Corrective Action

Restart nscd after any attribute change, using the following CLI command:

utils service restart Name Service Cache

CLI command to set TTL

Symptom

I used CLI command to set TTL for the nscd cache entries, but the value I set is not taking effect for A/AAAA record cache.

Corrective Action

The TTL configured for the A/AAAA record on the DNS server will override the configuration set for nscd.

The TTL configured for nscd will take effect only if TTL is not configured for the A/AAAA record on DNS server.

A/AAAA Record Queries before TTL expires

Symptom

Name Service Cache is enabled, I still see multiple A/AAAA record Queries sent to DNS Server before TTL expires.

Corrective Action

These queries are most likely triggered by nscd reloading the existing cache entries. Nscd reloading behavior is related to the reload-count in the nscd configuration file.

Clearing the cache

Symptom

Will restarting nscd clear the A/AAAA record cache?

Corrective Action

Restarting nscd does not always clear/flush the cache. It depends on the persistent attribute configuration.

- If the persistent attribute is set to Yes, the cache remains the same when nscd restarts.
- If the persistent attribute is set to No(default), the cache will be cleared/flushed when nscd restarts.

To clear/flush the cache, use the following CLI command:

admin:utils network name-service hosts cache invalidate

Content of AAAA record cache

Symptom

Can I see the content of A/AAAA record cache?

Corrective Action

No. NSCD activities can only be observed in nscd.log (with desired debugging level setting). A/AAAA record caching statistics can also be queried using the CLI command:

admin:show network name-service hosts cache-stats

Troubleshooting SAML Single Sign On

This section provides information on symptoms and corrective actions when SAML Single Sign On does not work as expected.

Redirection to IdP fails

Symptom

When the end users attempt to log into a SAML-enabled web application using a Unified Communications Manager supported web browser, they are not redirected to their configured Identity Provider (IdP) to enter the authentication details.

Corrective Action

Check if the following conditions are met:

- The IdP is up and running.
- The correct IdP metadata file is uploaded to Unified Communications Manager.
- Verify if the server and the IdP are part of the same circle of trust.

IdP Authentication Fails

Symptom

The end user is not getting authenticated by the IdP.

Corrective Action

Check if the following conditions are met:

- The LDAP directory is mapped to the IdP.
- The user is added to the LDAP directory.
- The LDAP account is active.
- The User Id and password are correct.

Redirection to Unified Communications Manager fails

Symptom

Even after getting authenticated by the IdP, the user is not redirected to SAML SSO enabled web applications.

Corrective Action

Check if the following conditions are met:

- The clocks of all the Unified Communications Manager nodes and the IdP are synchronized. See the NTP Settings section in System Configuration Guide for Cisco Unified Communications Manager for information on synchronizing clocks.
- The mandatory attribute uid is configured on the IdP.
- The correct Cisco Unified Communication server metadata file is uploaded to the IdP.
- The user has the required privileges.

Run Test Fails

Symptom

The Run test fails.

Corrective Action

Refer the corrective actions that are outlined in Redirection to IdP fails, on page 137, IdP Authentication Fails, on page 137, and Redirection to Unified Communications Manager fails, on page 138.

SAML Single Sign On Page Shows Incorrect Status on Cluster

Symptom

The SAML SSO is enabled on the cluster. If you disable SAML SSO on a subscriber while the publisher is down, and also disable SAML SSO on the publisher after the publisher is up, the clusterwide SAML SSO status is incorrectly displayed as 'SAML SSO enabled'.

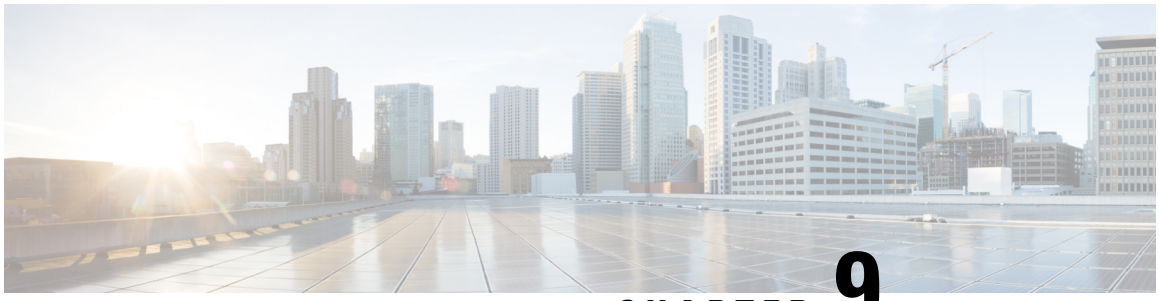
Corrective Action

View the 'Unified CM Cluster Overview' report in Cisco Unified Reporting. See the 'Unified CM SAML SSO Status Summary' section. This section indicates that the database value for SAML SSO status for a server is out of sync on the subscriber. Since the server reports that SAML SSO is enabled, the system assumes that the entire cluster is SAML SSO enabled. Restart that subscriber node to resolve this setting.

For more information about viewing reports in Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.

General Tips

- Be sure to set the SAML trace level to DEBUG. For more information on setting the SAML trace level, see *Command Line Interface Guide for Cisco Unified Communications Solutions, Release 10.0(1)*
- Collect the 'Cisco SSO' service logs (path: /tomcat/logs/ssosp/log4j/* and /platform/logs/ssoApp*) by using TLC in Unified RTMT or by executing the **CLI** command:**file get activelog**.



CHAPTER 9

SNMP Troubleshooting

This chapter provides information for use in SNMP troubleshooting.

- Troubleshooting Tips, on page 141
- CISCO-CCM-MIB Tips, on page 142
- HOST-RESOURCES-MIB Tips, on page 151
- CISCO-CDP-MIB Tips, on page 154
- SYSAPP-MIB Tips, on page 154
- SNMP Developer Tips, on page 156
- Where to Find More Information, on page 158

Troubleshooting Tips

Review this section for troubleshooting tips:

- Make sure that all the feature and network services that are listed in the SNMP Services section in the *Cisco Unified Serviceability Administration Guide* are running.
- Verify that the community string or SNMP user is properly configured on the system. You configure the SNMP community string or user by choosing **SNMP** > **V1/V2** > **Community String** or **SNMP** > **V3** > **User** in Cisco Unified Serviceability. Refer to *Cisco Unified Serviceability Administration Guide* for more information.

Cannot poll any MIBs from the system

This condition means that the community string or the SNMP user is not configured on the system, or they do not match with what is configured on the system.

Note By default, no community string or user gets configured on the system.

Check whether the community string or SNMP user is properly configured on the system by using the SNMP configuration windows.

Cannot receive any notifications from the system

This condition means that the notification destination is not configured correctly on the system.

Verify that you configured the notification destination properly in the Notification Destination (V1/V2c or V3) Configuration window.

Cannot receive SNMP traps from Unified Communications Manager node

This condition means that you cannot verify SNMP traps from the Unified Communications Manager node.

Verify that you configured the following MIB Object IDentifiers (OIDs) that relate to phone registration/deregistration/failure to the following values (the default for both values equals 0):

- ccmPhoneFailedAlarmInterval (1.3.6.1.4.1. 9.9.156.1.9.2) set to 30-3600. You can use this CLI command: **snmpset -c** <*community string*> **-v2c** <*transmitter ipaddress*> **1.3.6.1.4.1.9.9.156.1.9.2.0 i** <value>
- ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4) set to 30-3600. You can use this CLI command: **snmpset -c** <*community string*> **-v2c** <*transmitter ipaddress*> **1.3.6.1.4.1.9.9.156.1.9.4.0 i** <*value*>

Make sure that all the feature and network services that are listed in the SNMP Services section in the *Cisco Unified Serviceability Administration Guide* are running.

Verify that you configured the notification destination properly in the Notification Destination (V1/V2c or V3) Configuration window.

Verify that you configured the community string/user privileges correctly, including Notify permissions, in the Community String (V1/V2c) or User (V3) Configuration window.

CISCO-CCM-MIB Tips

This section contains tips for CISCO-CCM-MIB.

Related Topics

Frequently Asked Questions, on page 146
General Tips, on page 142
Limitations, on page 145

General Tips

- Be sure to set the trace setting to detailed for Cisco UCM SNMP Service (refer to the *Cisco Unified Serviceability Administration Guide*).
- Execute the command: **snmp walk -c** <*community*> **-v2c** <*ipaddress*> **1.3.6.1.4.1.9.9.156.1.1.2**
- Get the Unified Communications Manager version details
- Collect the following logs and information:
  - SNMP Master Agent (path: `platform/snmp/snmpdm/*`) and Cisco UCM SNMP Service (path: `cm/trace/ccmmib/sdi/*`) by using TLC in RTMT or this CLI command: **file get activelog**
  - SNMP package version by using this CLI command: **show packages active snmp**
  - MMF Spy output for phone by using this CLI command: **show risdb query phone**

- Send the trace logs and MMFSpy data for further analysis

The following table provides procedures for verifying that CISCO-CCM-MIB SNMP traps get sent.

Table 14: How to Check CISCO-CCM-MIB SNMP Traps

Trap	Verification Procedure
ccmPhoneStatusUpdate	**1.** Set MaxSeverity=Info in CiscoSyslog->dogBasic MIB table. **2.** Set PhoneStatusUpdateAlarmInterv=30 or higher in ccmAlarmConfigInfo MIB table. **3.** Disconnect the Unified Communications Manager server to which your phones register. **4.** Phones will unregister. **5.** Connect the Unified Communications Manager server again. **6.** Phones will re-register. **7.** Check that the ccmPhoneStatusUpdate trap is generated.
ccmPhoneFailed	**1.** Set MaxSeverity=Info in CiscoSyslog->clogBasic MIB table. **2.** Set PhoneFailedAlarmInterv=30 or higher in ccmAlarmConfigInfo MIB table. **3.** Make a phone fail. Delete a phone from Unified Communications Manager and register the phone again. **4.** Check that the ccmPhoneFailed trap is generated.

Trap	Verification Procedure
MediaResourceListExhausted	1. Create a Media Resource Group (MRG) that contains one of the standard Conference Bridge resources (CFB-2). 2. Create a Media Resource Group List (MRGL) that contains the MRG that was just created. 3. In the Phone Configuration window (for actual phones), set MRGL as the phone Media Resource Group List. 4. Stop the IPVMS, which makes the Conference Bridge resource(CFB-2) stop working. 5. If you make conference calls with phones that use the media list, you will see "No Conference Bridge available" on the phone screen. 6. Check that a MediaListExhausted Alarm/Alert/Trap is generated
RouteListExhausted	1. Create a Route Group (RG) that contains one gateway. 2. Create a Route Group List (RGL) that contains the RG that was just created. 3. Create a Route Pattern (9.XXXX) that routes a 9XXXX call through the RGL. 4. Unregister the gateway. 5. Dial 9XXXX on one of the phones. 6. Check that a RouteListExhausted Alarm/Alert/Trap gets generated.
MaliciousCallFailed	1. Create a softkey template. In the template, add the "MaliciousCall" softkeys to the different states for the phone. 2. Assign the new softkey template to actual phones; reset the phones. 3. Make some calls and select the "MaliciousCall" softkey in the phone screen during or after the call. 4. Check that a "MaliciousCallFailed" Alarm/Alert/Trap gets generated.

Collect the following logs and information for analysis:

- SNMP Master Agent logs stored at `/platform/snmp/snmpdm/*`.
- Cisco UCM SNMP Service by using the Real Time Monitoring Tool (RTMT) or by entering the **file get activelog** <*path*> CLI command. The path where the logs are stored is */cm/trace/ccmmib/sdi/**.
- All the files in /usr/local/Snmpri/conf folder. (Be aware that this is possible only if ROOT/REMOTE login is available.)
- The 'ls -l' listing of the preceding folder. (Be aware that this is possible only if ROOT/REMOTE login is available.)
- Perfmon logs by executing the **file get activelog /cm/log/ris/csv/** CLI command.
- Details of the set of actions that are performed that resulted in the issue.
- Ccmservice logs by executing the **file get activelog /tomcat/logs/ccmservice/log4j** CLI command.
- SNMP package version by execute the **show packages active snmp** CLI command.
- MMF Spy output for phone by executing the **show risdb query phone** CLI command.

Limitations

If multiple OIDs are specified in the SNMP request and if the variables are pointing to empty tables in CISCO-CCM-MIB, the request takes longer. In case the getbulk/getnext/getmany request has multiple OIDs in its request PDU with the subsequent tables being empty in the CISCO-CCM-MIB, the responses may specify NO_SUCH_NAME for SNMP v1 version or GENERIC_ERROR for SNMP v2c or v3 version.

- Reason—This timeout occurs due to the code that was added to enhance the performance of the CCMAgent and throttle when it gets a large number of queries, thus protecting the priority of Unified Communications Manager call processing engine.
- Workaround:
  - Use the available scalar variables (1.3.6.1.4.1.9.9.156.1.5) to determine the table size before accessing the table, or do the get operation on the desired table first and then query the nonempty tables.
  - Reduce the number of variables that are queried in a single request. For example, for empty tables. if Management application has timeout set at 3 seconds, Cisco recommends specifying no more than 1 OID. For nonempty tables, it takes 1 second to retrieve 1 row of data.
  - Increase the response timeout.
  - Reduce the number of retries.
  - Avoid using getbulk SNMP API. Getbulk API gets the number of records that is specified by MaxRepetitions. This means that even if the next object goes outside the table or MIB, it gets those objects. So, if the CISCO-CCM -MIB has empty tables, it goes to next MIB and this will need more time to respond. Use getbulk API when you know that the table is not empty and also know the number of records. Under this condition limit the max repetition counts to 5 to get response within 5 seconds.
  - Structure SNMP queries to adapt to current limits.
  - Avoid doing a number of getbulks on the PhoneTable in case a number of phones are registered to the Unified Communications Manager. In such a scenario, whenever an update occurs, ccmPhoneStatusUpdateTable gets updated.

Frequently Asked Questions

Why am I not getting any SNMP traps from the Unified Communications Manager node for the CISCO-CCM-MIB?

For receiving SNMP traps in CISCO-CCM-MIB, you need to ensure that the value of the following MIB OIDs is set to appropriate values: ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) and ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) are set between 30 and 3600. The default specifies zero (0).

Execute the following commands from any Linux machine:

- **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.156.1.9.2.0 i** <*value*>
- **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.156.1.9.4.0 i** <*value*>

The Following Issues Relate to Registration, Deregistration, and Failure of Phones

- Configuring notification destinations—You need to ensure that notification destinations are configured. You can do this from the Cisco Unified Serviceability Web window. A menu for **SNMP** > **Notification Destinations** exist.

  Before you configure notification destination, verify that the required SNMP services are activated and running (SNMP Master Agent and Cisco UCM SNMP Services). Also, make sure that you configured the privileges for the community string/user correctly, they should contain Notify permissions as well.

  If traps still are not generated, check whether corresponding alarms are generated. Because these traps get generated based on the alarm events, ensure that SNMP agents are getting these alarm events. Enable Local Syslog. Set up the Cisco UCM Alarm configuration to the informational level for Local Syslog destination from the Alarm configuration that is available on Cisco UCM Serviceability window **Alarm** > **Configuration**. Reproduce the traps and see whether corresponding alarms are logged into the CiscoSyslog file.

- Receiving syslog messages as traps—To receive syslog messages above a particular severity as traps, set the following 2 MIB objects in the clogBasic table:

  - clogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2)—Set this to **true** (**1**) to enable syslog trap notification. Default value specifies **false** (**2**). For example, **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.41.1.1.2.0 i** <*value*>.
  - clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3)—Set the severity level above which traps are desired. Default value specifies **warning** (**5**). All syslog messages with alarm severity lesser than or equal to configured severity level get sent as traps if notification is enabled. For example, **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.41.1.1.3.0 i** <*value*>

What are the different traps that are defined for Cisco Unified Communication Manager?

The CISCO-CCM-MIB contains the following list of defined traps:

- ccmCallManagerFailed—Indication that the Cisco UCM process detects a failure in one of its critical subsystems. It can also get detected from a heartbeat/event monitoring process.
- ccmPhoneFailed—Notification that the intervals that are specified in ccmPhoneFailedAlarmInterval indicate at least one entry in the ccmPhoneFailedTable.

- ccmPhoneStatusUpdate—Notification that gets generated at the intervals specified in ccmPhoneStatusUpdateInterv if there one entry in the ccmPhoneStatusUpdateTable exists.
- ccmGatewayFailed—Indication that at least one gateway attempted to register or communicate with the Cisco UCM and failed.
- ccmMediaResourceListExhausted—Indication that Cisco UCM has run out of a specified type of resource.
- ccmRouteListExhausted—Indication that the Cisco UCM could not find an available route in the indicated route list.
- ccmGatewayLayer2Change—Indication that the D-Channel/Layer 2 of a registered interface in a skinny gateway changes state.
- ccmMaliciousCall—Indication that a user registers a call as malicious with the local Cisco UCM server.
- ccmQualityReport—Indication that a user reports a quality problem using the Quality Report Tool.
- ccmTLSConnectionFailure—Indication that the Unified Communications Manager failed to open TLS connection for the indicated device.

The mapping of the traps to alarms follows:

- ccmCallManagerFailed—CallManagerFailure
- ccmPhoneFailed—DeviceTransientConnection
- ccmPhoneStatusUpdate
- ccmGatewayFailed—DeviceTransientConnection
- ccmMaliciousCall—MaliciousCall
- ccmMediaResourceListExhausted—MediaResourceListExhausted
- ccmQualityReportRequest—QRTRequest
- ccmRouteListExhausted—RouteListExhausted
- ccmGatewayLayer2Change—DChannelOOS, DChannelISV

How can different SNMP traps from Cisco Unified Communication Manager be checked?

Use the following procedure for triggering few traps:

- ccmPhoneStatusUpdate trap
  - Set ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) to 30 or higher in ccmAlarmConfigInfo MIB table.
  - Disconnect the Unified Communications Manager server where your phones are registered. Phones will unregister.
  - Connect the Unified Communications Manager server again. Phones will re-register and you will get the ccmPhoneStatusUpdate trap.
- ccmPhoneFailed trap

- Set ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) to 30 or higher in ccmAlarmConfigInfo MIB table.
- Make a phone fail. Delete a phone from Unified Communications Manager and register the phone again. For phone failed traps, you can try two different scenarios:

  Set the phone to point to tftp/Unified Communications Manager server A. Plug the phone into Unified Communications Manager server B on different switch. The phone status remains unknown. You will see following message:

```
2007-10-31:2007-10-31 14:53:40 Local7.Debug 172.19.240.221 community=public,
 enterprise=1.3.6.1.4.1.9.9.156.2.0.2, enterprise_mib_name=ccmPhoneFailed,
 uptime=7988879, agent_ip=128.107.143.68, version=Ver2,
ccmAlarmSeverity=error, ccmPhoneFailures=1.
```

  Register a 7960 phone as a 7940 phone in the Cisco UCM and cause the db issue that generates the phone fail trap.

- MediaResourceListExhausted trap
  - Create a Media Resource Group (MRG) and have it contain one of the standard ConferenceBridge resources (CFB-2).
  - Create a Media Resource Group List (MRGL) and have it contain the MRG just created.
  - In the Phone Configuration window for real phones, set MRGL as the phone Media Resource Group List.
  - Stop the IPVMS, which makes the ConferenceBridge resource (CFB-2) stop working.
  - Make conference calls with phones by using the media list; you will see No Conference Bridge available on the phone screen.
  - Check whether a MediaListExhausted alarm/alert/trap gets generated.
- RouteListExhausted trap
  - Create a Route Group (RG) and have it contain one gateway.
  - Create a Route Group List (RGL) and have it contain the RG just created.
  - Create a Route Pattern (9.XXXX) that reroutes a 9XXXX call through the RGL.
  - Unregister the gateway.
  - Dial 9XXXX on one of the phones.
  - Check whether a RouteListExhausted alarm/alert/trap gets generated.
- MaliciousCallFailed trap
  - Create a softkey template. In the template, add all available MaliciousCall softkeys to the phone status.
  - Assign the new softkey template to real phones; reset the phones.
  - Make calls and select the MaliciousCall in the phone screen during or after the call.
  - Check whether a MaliciousCallFailed alarm/alert/trap gets generated.

- GatewayFailed trap
  - Method 1: Remove the gateway configuration from the database by using Web Admin or change the gateway MAC address to an invalid value and update. Reboot the gateway. Or restart the Cisco UCM service to which the gateway is connected.
  - Method 2: Set GatewayAlarmEnable=true in ccmAlarmConfigInfo MIB table. In Cisco Unified Serviceability, go to the SNMP configuration window to ensure that you have the SNMP community string and trap destination set correctly. Create a gateway failure event and the trap gets displayed on the trap receiver. To cause a gateway failure and failover, restart Cisco UCM. The gateway fails over to the redundant Cisco UCM server. The gateway should not be configured in the database on the redundant Cisco UCM server.
- ccmGatewayLayer2Change trap
  - ccmGatewayLayer2Change trap gets triggered during D-Channel Out of service (DChannelOOS) or D-Channel Inservice (DChannelISV) from Cisco UCM. Check whether any such events gets triggered for testing purposes.
- ccmCallManagerFailed trap
  - The Cisco UCM failed alarm gets generated when an internal error occurs. These alarms include an internal thread dying due to lack of CPU, timer issues, and other issues. This trap would represents something that is hard to reproduce unless the Cisco UCM team intentionally causes one of these occurrences.

If the Cisco UCM Agent consumes high CPU continuously, what needs to be done?

Collect logs for analysis and refer to defect CSCsm74316. Verify whether the defect fix was added to your Cisco UCM release.

If the CTI Routepoint is deleted from Unified Communications Manager Administration, an entry exists for that in ccmCTIDeviceTable mib. Why?

A service parameter that is called “RIS Unused Cisco CallManager Device Store Period” defines how long unregistered devices remain in RIS database and in the MIB. The Cisco UCM Administration window and the SNMP MIB may not be in sync because the Cisco UCM Administration window shows information from the database and SNMP uses the RIS database.

When ccmPhoneType is queried from ccmPhoneTable in Cisco-CCM-MIB, no information is returned. Why?

This means that the ccmPhoneType has been obsoleted. You can retrieve the same information from ccmPhoneProductTypeIndex against CcmProductTypeEntry. In the table, the indexes correspond to the index and name as listed in that table.

The following list gives some of other obsolete and alternate OIDs to be referred:

- Because ccmGatewayType is obsolete, you need to refer to ccmGateWayProductTypeIndex.
- Because ccmMediaDeviceType is obsolete, you need to refer to ccmMediaDeviceProductTypeIndex.
- Because ccmCTIDeviceType is obsolete, you need to refer to ccmCTIDeviceProductTypeIndex.

A query on ccmPhoneProductTypeIndex returns zero. Why?

Verify that the Unified Communications Manager release that you are using has this capability.

While a WALK is performed on ccmPhoneTable, ccmPhoneUserName is not returning any value. How are usernames associated to the IP phones?

Create an end user and go to the phone that has been registered and associate the Owner User ID. After this is done, the OID in the SNMP Walk will show the user.

How do I get the firmware versions of each phone by using SNMP?

ccmPhoneLoadID object in the ccmPhoneTable will give the firmware version of each phone. This value may differ if new image download failed because SNMP exposes both configured firmware ID (ccmPhoneLoadID) and the actual running firmware (ccmPhoneActiveLoad).

CCM MIB returns ccmVersion as 5.0.1, which is incorrect.

Verify the Unified Communications Manager release that you are using has this capability. If it does not, upgrade.

CCM MIB returns incorrect ccmPhoneLoadID

ccmPhoneLoadID values get picked up from the RIS database, which gets populated based on the alarm that is received during phone registration. Perform the following steps and collect the logs for further analysis:

1. In Cisco Unified Serviceability, choose **Alarm** > **Configuration**. Choose the server; then, click **Go**. Choose **CM Services** for the Services Group; then, click **Go**. Choose **Cisco CallManager** for the service; then, click **Go**.
2. Check **Enable Alarm** for Local Syslog, SDI Trace, and SDL Trace. Choose **Informational** from each Alarm Event Level drop-down list box.
3. In the Trace Configuration window, set the Debug Trace Level for the Cisco UCM service to **Detailed**.
4. Reset the phones that are showing incorrect LoadID.
5. Collect the Syslog and Cisco UCM traces.
6. Collect the phone details.

How Cisco Call Manager status (START/STOP) monitored?

For service monitoring, you have following options:

- SYSAPPL MIB
- HOST-RESOURCE-MIB
- CISCO-CCM-MIB (ccmStatus)
- SOAP interface
- Real-Time Monitoring Tool (RTMT) alerts

A ccmCallManagerFailed trap exists for Cisco UCM service failures. But this does not cover normal service stop and unknown crashes.

Why does the device pool information seem incorrect for any device that was polled? The OID that was used is ccmPhoneDevicePoolIndex.

As stated in the CISCO-CCM-CAPABILITY MIB, ccmPhoneDevicePoolIndex does not get supported, so it returns zero (0). The Cisco UCM device registration alarm currently does not contain the device pool information.

HOST-RESOURCES-MIB Tips

HOST-RESOURCES-MIB retrieves information about all the processes that are running on the system from hrSWRunTable. Use the HOST-RESOURCES-MIB when you want to monitor all the processes that are running in the system. To monitor only the installed Cisco application, use SYSAPPL-MIB.

Related Topics

Disk Space and RTMT, on page 151
Frequently Asked Questions, on page 152
Logs for Collection, on page 151

Logs for Collection

Collect the following logs and information for troubleshooting purposes:

- The hostagt log files by executing the **file get activelog /platform/snmp/hostagt/** command.
- The syslog files by executing the **file get activelog /syslog/** command.
- Master SNMP Agent log files by executing the **file get activelog /platform/snmp/snmpdm/** command.
- Sequence of operations performed.

Disk Space and RTMT

The used and available disk space values that are shown by HOST-RESOURCES-MIB may not match the disk space values that are shown by RTMT due to the minfree percentage of reserved file system disk blocks. Because the minfree value for Unified Communications Manager in Release 7.1(x) and later systems equals 1 percent, you will see a 1-percent difference between the used disk space value that is shown by RTMT and HOST-RESOURCES-MIB.

- In RTMT, the disk space used value gets shown from df reported values: [(Total Space – Available Space) /Total Space] * 100 where the Total Space includes the minfree also.
- For Host Resources MIB, the disk space used value gets calculated by [hrStorageUsed/hrStorageSize] * 100 where the hrStorageSize does not include the minfree.

Frequently Asked Questions

Can the HOST-RESOURCES-MIB be used for process monitoring?

Host resources MIB does retrieve the information about the processes that are running on the system in hrSwRunTable; however, this monitors all the processes that are running in the system. If you need to monitor only the installed Cisco Application, the best way requires you to use SYSAPPL-MIB.

How are the memory usage values that are shown by Real-Time Monitor Tool mapped to the HOST-RESOURCES-MIB?

The following table lists the memory usage values.

Table 15: Memory Usage Values

Memory Usages	RTMT Counter	HOST-RESOURCES-MIB
SWAP memory Usage	Memory\Used Swap Kbytes	hrStorageUsed.2 (whose description is virtual memory)
Physical Memory Usage	Memory\Used Kbytes	hrStorageUsed.1(whose description is Physical RAM)
Total memory (physical + swap) usage	Memory\Used VM Kbytes	No equivalent. Basically need to add hrStorageUsed.2 and hrStorageUsed.1 Because you cannot use swap memory at all on lightly used servers, HR Virtual Memory may return 0. To validate HR VM is returning correctly, you need to compare the value against RTMT Memory\Used Swap KBytes. RTMT and HR use the term “Virtual memory” differently. The hrStorageUsed for physical memory shows the data in terms of used - (buffers + cache). The hrStorageUsed for physical memory shows the data in terms of used that is buffers + cache. The shared memory information that is exposed by the HOST-RESOURCES-MIB is ::hrStorageDescr.10 = STRING: /dev/shm. The virtual memory that gets reported by HOST-RESOURCES-MIB comprises what is considered as swap memory by RTMT. For HOST RESOURCES MIB, the following formula gets used: • %Physical memory usage = (Physical RAM hrStorageUsed + /dev/shm hrStorageUsed) / (Physical RAM hrStorageSize) • %VM used = (Physical RAM hrStorageUsed + /dev/shm hrStorageUsed + Virtual Memory hrStorageUsed) / (Physical RAM hrStorageSize + Virtual Memory hrStorageSize)

Why do the disk space values shown by RTMT and the HOST-RESOURCES-MIB differ?

In general, the df size will not match the used and available disk space data shown. This occurs because of minfree percentage of reserved filesystem disk blocks. The minfree value for a Cisco Unified Communication Manager in Releases 6.x and 7.0 is 1percent. The difference of 1 percent occurs between the disk space used value that is shown in RTMT and HOST-RESOURCES-MIB.

In RTMT, the disk space used value gets shown from df reported values: [(Total Space - Available Space) /Total Space] * 100 where the Total Space includes the minfree also. For the HOST-RESOURCES-MIB, this gets calculated by [hrStorageUsed/hrStorageSize] * 100 wherein the hrStorageSize does not include the minfree.

How does the Host Agent display the value in hrStorageUsed?

The hrStorageUsed for physical RAM got corrected to show the data in terms of used (buffers + cache). To check whether the host agent version is correct, collect the snmp-rpm version that is installed in the system by using the **show packages active snmp** command.

How the Memory Capacity/Usage Values compare to those of HOST-RESOURCES-MIB?

In the HOST-RESOURCES-MIB, the size and storage used get represented in terms of hrStorageUnits. If, for that storage type, the hrStorageUnits equals 4096 bytes, the hrStorageUsed or hrStorageSize value queried in the MIB value should get multiplied by 4096. For example, by using the **show status** command, the Total Memory displays as 4090068K for Physical RAM.

If the hrStorageUnits for physicalRAM storage type equals 4096 bytes, the hrStorageSize for Physical RAM will get shown as 1022517, which is 4090078K [(1022517 x 4096)/1024 = 4090068K].

Why does an SNMP query on hrSWRunName in HOST-RESOURCES-MIB intermittently return incorrect entries in Windows?

The Microsoft SNMP extension agent (hostmib.dll) supports the HOST-RESOURCE-MIB. Microsoft support may be able to help on this. If the problem is persistent, perform the following steps:

1. Use the tlist snmp.exe file to verify that the hostmib.dll is listed in the output.
2. Verify that no error/warning messages from SNMP exist in the event viewer when SNMP service is started.
3. Make sure that the community string used has been configured with read privilege under snmp service properties.
4. Use MSSQL-MIB (MssqlSrvInfoTable) to confirm SQL process status.

Monitoring Processes

HOST-RESOURCES-MIB retrieves information about all the processes that are running on the system from hrSWRunTable. Use this MIB for monitoring all the processes that are running in the system. To monitor only the installed Cisco application, use SYSAPPL-MIB.Disk Space and RTMT.

The used and available disk space values that are shown by HOST-RESOURCES-MIB may not match the disk space values that are shown by RTMT due to the minfree percentage of reserved file system disk blocks. Because the minfree value for Unified Communications Manager in 6.x and 7.0 systems equals 1 percent, you will see a 1-percent difference between the used disk space value that is shown by RTMT and HOST-RESOURCES-MIB.

- In RTMT, the disk space used value gets shown from df reported values: [(Total Space – Available Space) /Total Space] * 100 where the Total Space includes the minfree also.
- For Host Resources MIB, the disk space used value gets calculated by [hrStorageUsed/hrStorageSize] * 100 where the hrStorageSize does not include the minfree.

CISCO-CDP-MIB Tips

This section contains the following topics:

Related Topics

Frequently Asked Questions, on page 154
General Tips, on page 154

General Tips

Collect the following logs and information for analysis:

- Use the **set trace enable Detailed cdpmib** command to set the detailed trace for cdpAgt ().
- Restart the Cisco CDP Agent service from the Cisco Unified Serviceability window (**Tools** > **Control Center** > **Network Services**) and wait for some time.
- Collect the following trace files:
  - Enable the Cisco CDP Agent traces by using the **file get activelog cm/trace/cdpmib/sdi** command and Cisco CDP daemon traces by using the **file get activelog cm/trace/cdp/sdi** command.
  - Enable the Cisco CDP Agent and daemon traces by using the Real-Time Monitoring Tool (RTMT) **Trace & Log Central** > **Collect Files** > **Cisco CallManager SNMP Service** > **Cisco CDP Agent and Cisco CDP**.
- After the logs are collected, reset the trace setting by using the **set trace disable cdpmib** command.

Frequently Asked Questions

Why are the CDP interface table and globalinfo tables are blank?

Verify that your Cisco UCM release has this capability. If not, upgrade.

How is the MessageInterval value set in the Interface table as well as Global table in CDP MIB?

Check to see whether the HoldTime value is greater than MessageInterval value. If it is less, the MessageInterval value cannot get set from both interface table and global table.

SYSAPP-MIB Tips

This section contains tips for SYSAPP-MIB.

Related Topics

Collecting Logs, on page 155
Using Servlets in Cisco Unified Communications Manager 8.0, on page 155

Collecting Logs

Collect the following logs and information for analysis. Execute the command **file get activelog** <*paths in the following bullets*>

- SNMP Master Agent Path: `/platform/snmp/snmpdm/*`
- System Application Agent Path: `/platform/snmp/sappagt/*`

Using Servlets in Cisco Unified Communications Manager 8.0

The SysAppl MIB provides a way to get inventory of what is installed and running at a given time. SysAppl agent cannot give the list of services that are activated or deactivated. It can only provide the running/not running states of the application/services. Web App services/Servlets cannot get monitored by using the SysAppl MIB. The following servlets exist for a 8.0 system:

- Cisco CallManager Admin
- Cisco CallManager Cisco IP Phone Services
- Cisco CallManager Personal Directory
- Cisco CallManager Serviceability
- Cisco CallManager Serviceability RTMT
- Cisco Dialed Number Analyzer
- Cisco Extension Mobility
- Cisco Extension Mobility Application
- Cisco RTMT Reporter Servlet
- Cisco Tomcat Stats Servlet
- Cisco Trace Collection Servlet
- Cisco AXL Web Service
- Cisco Unified Mobile Voice Access Service
- Cisco Extension Mobility
- Cisco IP Manager Assistant
- Cisco WebDialer Web Service
- Cisco CAR Web Service
- Cisco Dialed Number Analyzer

For monitoring important service status for system health purposes, Cisco recommends the following approaches:

- Use the Cisco Unified Serviceability API that is called GetServiceStatus. This API can provide complete status information, including activation status for both web application type and non web app services. (See *AXL Serviceability API Guide* for more details.)
- Use the **utils service list** command to check the status of different services.
- Use the Syslog message and monitor the servM generated messages. For example:

```
Mar 18 16:40:52 ciscart26 local7 6 : 92: Mar 18 11:10:52.630 UTC :
%CCM_SERVICEMANAGER-SERVICEMANAGER-6-ServiceActivated: Service Activated.
Service Name:Cisco CallManager SNMP Service App ID:Cisco Service Manager
Cluster ID: Node ID:ciscart26
```

SNMP Developer Tips

Review this section for SNMP developer troubleshooting tips:

- Refer to the CISCO-CCM-CAPABILITY-MIB at the following link for the support list for CISCO-CCM-MIB:

  http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

  CISCO-CCM-CAPABILITY

  As stated in the CISCO-CCM-CAPABILITY-MIB, ccmPhoneDevicePoolIndex does not get supported, so it returns a 0. The Cisco UCM device registration alarm currently does not contain the device pool information.

- If Cisco UCM SNMP service is not running, only the following tables in the MIB will respond:
  - ccmGroupTable
  - ccmRegionTable
  - ccmRegionPairTable
  - ccmDevicePoolTable
  - ccmProductTypeTable
  - ccmQualityReportAlarmConfigInfo
  - ccmGlobalInfo

    To get Cisco UCM SNMP service running, activate and start the service in Cisco Unified Serviceability.

- Query the SysApplInstallPkgTable in SYS-APPL MIB to get an inventory of Unified Communications Manager applications that are installed on the system. Query the SysApplRunTable in SYS-APPL MIB to get an inventory of Unified Communications Manager applications that are running on the system. Because System Application Agent cannot show services that are activated and deactivated or monitor

Web App services or servlets, use this approach to monitor system health and service status for Unified Communications Manager applications:

- Use the Cisco Unified Serviceability API that is called getservicestatusto provide complete status information, including activation status, for both Web applications and non-Web applications. See the AXL Serviceability API Guide for more details.
- Check service status with this CLI command: **utils service list**
- Monitor the servM-generated messages with Syslog (see the following example):

```
Mar 18 16:40:52 ciscart26 local7 6 : 92: Mar 18 11:10:52.630 UTC :
%CCM_SERVICEMANAGER-SERVICEMANAGER-6-ServiceActivated: Service Activated.
 Service Name:Cisco CallManager SNMP Service App ID:Cisco Service Manager
 Cluster ID: Node ID:ciscart26
```

Note Unified Communications Manager uses the following Web application services and servlets: Cisco UCM Admin, Cisco UCM Cisco IP Phone Services, Cisco UCM Personal Directory, Cisco Unified Serviceability, Cisco Unified RTMT, Cisco Extension Mobility, Cisco Extension Mobility Application, Cisco Unified RTMT Reporter Servlet, Cisco Tomcat Stats Servlet, Cisco Trace Collection Servlet, Cisco AXL Web Service, Cisco Unified Mobile Voice Access Service, Cisco Extension Mobility, Cisco IP Manager Assistant, Cisco WebDialer Web Service, Cisco CAR Web Service, and Cisco Dialed Number Analyzer.

Request Timeout Workaround

If an SNMP request specifies multiple OIDs and the variables are pointing to empty tables, you may get a NO_SUCH_NAME (for SNMP V1) or GENERIC ERROR (for SNMP V2c or V3) due to a timeout problem. A timeout can occur as a result of throttling enhancements to protect the Unified Communications Manager processing engine.

Note You can retrieve the count of entries in CCMH323DeviceTable and ccmSIPDeviceTable by using scalar objects, so the SNMP Manager (the client) can avoid unnecessary **get/getnext** operations on these tables when no entries exist.

As an SNMP developer, you can use the following workaround for this problem:

- First, use the available scalar variables (1.3.6.1.4.1.9.9.156.1.5) to determine table size before accessing the table or perform the **get** operation on the desired table; then, query the non-empty tables.
- Reduce the number of variables that are queried in a single request; for example, for empty tables, if the management application has the timeout set to 3 seconds, specify only 1 OID. (For non-empty tables, it takes 1 second to retrieve one row of data.)
- Increase the response timeout.
- Reduce the number of retries.
- Avoid using getbulk SNMP API. The getbulk API retrieves the number of records that is specified by MaxRepetitions, so even if the next object goes outside the table or MIB, it gets those objects. Empty

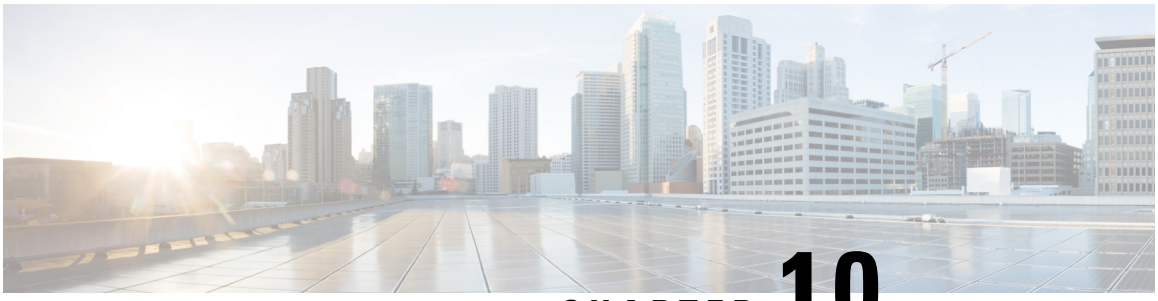
tables cause even more delay. Use getbulk API for non-empty tables with a known number of records. In these circumstances, set MaxRepetitions to 5 seconds to require a response within 5 seconds.

- Structure SNMP queries to adapt to existing limits.
- Avoid performing multiple getbulks to walk the PhoneTable periodically in case a large number of phones are registered to Cisco UCM. You can use the ccmPhoneStatusUpdateTable, which updates whenever there is a Phone update, to decide whether to walk the PhoneTable.

Where to Find More Information

Related Documentation

- *Command Line Interface Reference Guide for Cisco Unified Solutions*
- "SNMP" chapter, *Cisco Unified Serviceability Administration Guide*



CHAPTER 10

Opening a Case With TAC

This section contains details on the type of information that you need when you contact TAC and information on methods of sharing information with TAC personnel.

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website remains available 24 hours a day, 365 days a year at this URL: *http://www.cisco.com/techsupport*

Using the online TAC Service Request Tool represents the fastest way to open S3 and S4 service requests. (S3 and S4 service requests specify those requests in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved by using the recommended resources, your service request will get assigned to a Cisco TAC engineer. Find the TAC Service Request Tool at this URL: *http://www.cisco.com/techsupport/servicerequest*

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests represent those in which your production network is down or severely degraded.) Cisco TAC engineers get assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL: *http://www.cisco.com/techsupport/contacts*

- Information You Will Need, on page 160
- Required Preliminary Information, on page 160
- Online Cases, on page 162
- Serviceability Connector, on page 162
- Cisco Live!, on page 163
- Remote Access, on page 163
- Cisco Secure Telnet, on page 164
- Set up a Remote Account, on page 165

Information You Will Need

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 until you have an engineer request after opening a case inevitably results in resolution delay.

Related Topics

Cisco Live!, on page 163
Cisco Secure Telnet, on page 164
General Information, on page 161
Network Layout, on page 160
Online Cases, on page 162
Problem Description, on page 161
Remote Access, on page 163
Required Preliminary Information, on page 160

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.

Related Topics

General Information, on page 161
Network Layout, on page 160
Problem Description, on page 161

Network Layout

Provide a detailed description of the physical and logical setup, as well as all the following network elements that are involved in the voice network (if applicable):

- Unified Communications Manager(s)
  - Version (from Unified Communications Manager Administration, choose **Details**)
  - Number of Unified Communications Managers
  - Setup (stand alone, cluster)
    - Unity
  - Version (from Unified Communications Manager Administration)
  - Integration type
    - Applications
  - List of installed applications

- Version numbers of each application
    - IP/voice gateways
- OS version
- Show tech (IOS gateway)
- Unified Communications Manager 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 Unified Communications Manager 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)?

Online Cases

Opening a case online through Cisco.com gives it initial priority over all other case-opening methods. High-priority cases (P1 and P2) provide an exception to this rule.

Provide an accurate problem description when you open a 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.

Serviceability Connector

Serviceability Connector Overview

You can ease the collection of logs with the Webex Serviceability service. The service automates the tasks of finding, retrieving, and storing diagnostic logs and information.

This capability uses the *Serviceability Connector* deployed on your premises. Serviceability Connector runs on a dedicated host in your network ('connector host'). You can install the connector on either of these components:

- Enterprise Compute Platform (ECP)—Recommended

  ECP uses Docker containers to isolate, secure, and manage its services. The host and the Serviceability Connector application install from the cloud. You don’t need to manually upgrade them to stay current and secure.

Important We recommend use of ECP. Our future development will focus on this platform. Some new features won't be available if you install the Serviceability Connector on an Expressway.

- Cisco Expressway

You can use the Servicability Connector for these purposes:

- Automated log and system information retrieval for service requests
- Log collection of your Unified CM clusters in a Cloud-Connected UC deployment

You can use the same Serviceability Connector for both use cases.

Benefits of Using Serviceability Service

The service offers these benefits:

- Speeds up the collection of logs. TAC engineers can retrieve relevant logs as they perform the diagnosis of the problem. They can avoid the delays of requesting extra logs and waiting for their manual collection and delivery. This automation can take days off your problem resolution time.

- Works with TAC's Collaboration Solution Analyser and its database of diagnostic signatures. The system automatically analyses logs, identifies known issues, and recommends known fixes or workarounds.

TAC Support for Serviceability Connector

For more details on Serviceability Connector, see https://www.cisco.com/go/serviceability or contact your TAC representative.

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 you are 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 get made to the system without customer consent.

Cisco Secure Telnet

Cisco Secure Telnet offers Cisco Service Engineers (CSE) transparent firewall access to Unified Communications Manager 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 Unified Communications Manager 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.

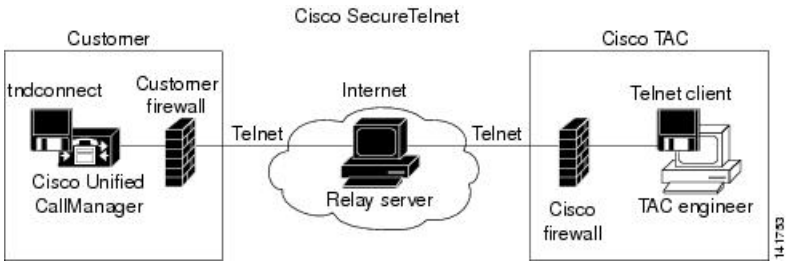
Corporate networks normally permit communication with the public Internet but only if connections directed to outside hosts originate from inside the firewall.

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 secure communication between the shielded remote systems get supported.

Figure 1: Cisco Secure Telnet System



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 Unified Communications Manager 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 that run on Windows NT and Windows 2000 or with UNIX operating systems.

After the Cisco Communications Manager 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.

After the Telnet connection is stable, the CSE can implement all remote serviceability functionality to perform maintenance, diagnostic, and troubleshooting tasks on your Unified Communications Manager server.

You can view the commands that the CSE sends and the responses that your Unified Communications Manager server issues, but the commands and responses may not always be completely formatted.

Set up a Remote Account

Configure a remote account in the Unified Communications Manager so that Cisco support can temporarily gain access to your system for troubleshooting purposes.

Procedure

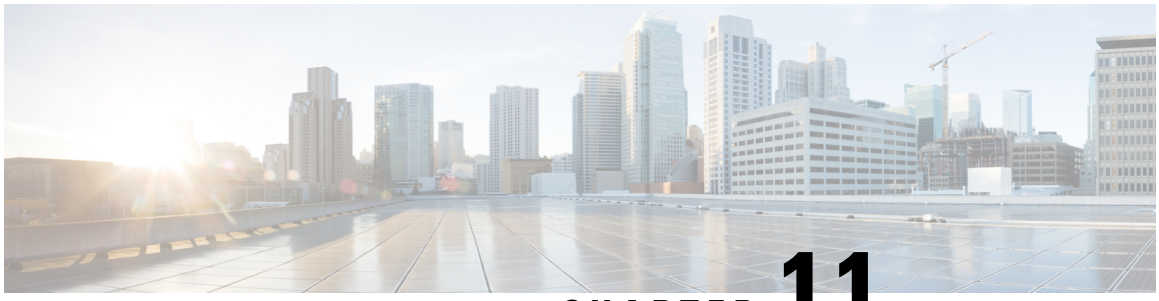
Step 1 From Cisco Unified Operating System Administration, choose **Services** > **Remote Support**.

Step 2 In the **Account Name** field, enter a name for the remote account.

Step 3 In the **Account Duration** field, enter the account duration in days.

Step 4 Click **Save**.
The system generates an encrypted pass phrase.

Step 5 Contact Cisco support to provide them with the remote support account name and pass phrase.



CHAPTER 11

Case Study: Troubleshooting Cisco Unified IP Phone Calls

This appendix contains two case studies for troubleshooting Cisco Unified IP Phones.

- Troubleshooting Intracluster Cisco Unified IP Phone Calls, on page 167
- Troubleshooting Intercluster Cisco Unified IP Phone Calls, on page 175

Troubleshooting Intracluster Cisco Unified IP Phone Calls

The case study in this section discusses in detail the call flow between two Cisco Unified IP Phones within a cluster, called an intracluster call. This case study also focuses on Unified Communications Manager and Cisco Unified IP Phone initialization, registration, and keepalive processes. A detailed explanation of an intracluster call flow follows the discussion.

Related Topics

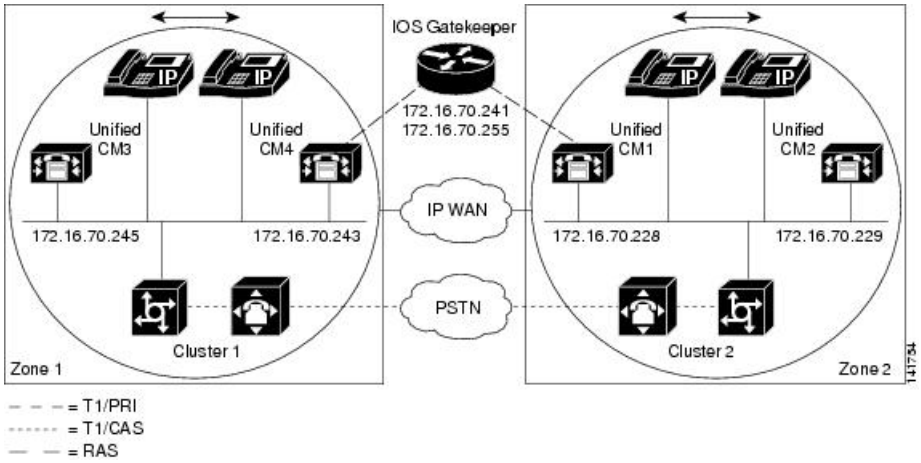
Cisco Unified Communications Manager Initialization Process, on page 169
Cisco Unified Communications Manager Intracluster Call Flow Traces, on page 171
Cisco Unified Communications Manager KeepAlive Process, on page 171
Cisco Unified Communications Manager Registration Process, on page 170
Cisco Unified IP Phone Initialization Process, on page 168
Sample Topology, on page 167
Self-Starting Processes, on page 169
Troubleshooting Tools, on page 5

Sample Topology

You have two clusters that are named Cluster 1 and Cluster 2; the two Unified Communications Managers in Cluster 1 are called Unified CM3 and Unified CM4, while the two Unified Communications Managers in Cluster 2 are called Unified CM1 and Unified CM2.

The traces that are collected for this case study come from Unified CM1, which is located in Cluster 2, as shown in the following figure. The two Cisco Unified IP Phones in Cluster 2 provide the basis for the call flow. The IP addresses of these two Cisco Unified IP Phones specify 172.16.70.230 (directory number 1000) and 172.16.70.231 (directory number 1001), respectively.

Figure 2: Sample Topology of Intracluster Cisco Unified IP Phone-to-Cisco Unified IP Phone Calls



Cisco Unified IP Phone Initialization Process

The following procedure explains in detail the Cisco Unified IP Phone initialization (or boot up) process.

Procedure

1. If you have set the appropriate options in DHCP server (such as Option 066 or Option 150), the Cisco Unified 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).
2. If DHCP sends a DNS name of the TFTP sever, 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.
3. If the DHCP reply does not include a TFTP server name, the Cisco Unified IP Phone uses the default server name.
4. The configuration file (.cnf) gets retrieved from the TFTP server. All.cnf files have the name SEP<mac_address>.cnf. If this is the first time that the phone is registering with the Unified Communications Manager, a default file, SEPdefault.cnf, gets downloaded to the Cisco Unified IP Phone. In this case study, the first Cisco Unified IP Phone uses the IP address 172.16.70.230 (its MAC address is SEP0010EB001720), and the second Cisco Unified IP Phone uses the IP address 172.16.70.231 (its MAC address is SEP003094C26105).
5. All.cnf files include the IP address(es) for the primary and secondary Unified Communications Manager(s). The Cisco Unified IP Phone uses this IP address to contact the primary Unified Communications Manager and to register.
6. After the Cisco Unified IP Phone connects and registers with Unified Communications Manager, the Unified Communications Manager tells the Cisco Unified IP Phone which executable version (called a load ID) to run. If the specified version does not match the executing version on the Cisco Unified IP Phone, the Cisco Unified IP Phone will request the new executable from the TFTP server and reset automatically.

Cisco Unified Communications Manager Initialization Process

This section explains the initialization process of Unified Communications Manager with the help of traces that are captured from Unified Communications Manager1 (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 that is sent between endpoints.

This section describes the events that occur when Unified Communications Manager is initialized. Understanding how to read traces will help you to properly troubleshoot the various Unified Communications Manager processes and the effect of those processes on services such as conferencing and call forwarding.

The following messages from the Unified Communications Manager SDI trace utility show the initialization process on one of the Unified Communications Managers, in this case, Unified Communications Manager1.

- The first message indicates that Unified Communications Manager started its initialization process.
- The second message indicates that Unified Communications Manager read the default database values (for this case, it is the primary or publisher database).
- The third message indicates Unified Communications Manager received the various messages on TCP port 8002.
- The fourth message shows that, after receiving to these messages, Unified Communications Manager added a second Unified Communications Manager to its list: Unified CM2 (172.16.70.229).
- The fifth message indicates that Unified Communications Manager has started and is running Unified Communications Manager version 3.1(1).

```
16:02:47.765 CCM|CMProcMon - Communications ManagerState Changed -
Initialization Started.16:02:47.796 CCM|NodeId:  0, EventId: 107 EventClass:
 3 EventInfo: Cisco CCMDatabase 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

After Unified Communications Manager 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 that the messages that are described during these processes are very useful when you are troubleshooting a problem that is related to the features in Unified Communications Manager.

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 Unified Communications Manager started RoutePlanManager and if it is trying to load the RouteLists. The following sample configuration shows that RouteListName=“ipwan” and RouteGroupName=“ipwan” are loading and starting.

```
16:02:51.031 CCM|MulicastPointManager - Started16:02:51.031
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 that is adding the device 172.16.70.245, which is Unified CM3 that is located in Cluster 1 and is considered an H.323 device. In this case, the RouteGroup gets created to route calls to Unified CM3 in Cluster 1 with Cisco IOS Gatekeeper permission. If a problem occurs while the call is being routed to a Cisco Unified IP Phone that is 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 Unified Communications Manager is adding "Dns" (Directory Numbers). By reviewing these messages, you can determine whether the Unified Communications Manager read the directory number from the database.

```
16:02:51.671 CCM|NodeId:    1, EventId: 1540 EventClass:  2 EventInfo: Call control
 started16:02:51.843 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 Unified Communications Manager 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 Unified Communications Manager in a different cluster. That Unified Communications Manager gets registered as an H.323 Gateway with this Unified Communications Manager.

```
16:02:52.250 CCM|DeviceManager: Statically Initializing Device;
DeviceName=172.16.70.22616:02:52.250 CCM|DeviceManager: Statically Initializing
Device;  DeviceName=172.16.70.245
```

Cisco Unified Communications Manager Registration Process

Another important part of the SDI trace involves the registration process. When a device is powered up, it gets information using DHCP, connects to the TFTP server for its.cnf file, and then connects to the Unified Communications Manager that is specified in the.cnf file. The device could be an MGCP gateway, a Skinny gateway, or a Cisco Unified IP Phone. Therefore, you need to be able to discover whether devices successfully registered on the Cisco network.

In the following trace, Unified Communications Manager received new connections for registration. The registering devices comprise MTP_nsa-cm1 (MTP services on Unified CM1) and CFB_nsa-cm1 (Conference Bridge service on Unified CM1). Although these are software services that are running on Unified Communications Manager, 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-cm1, 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-cm1, TCPHandle=0x4fe05e8, Socket=0x59c, IPAddr=172.16.70.228,
 Port=3280, StationD=[1,96,2]
```

Cisco Unified Communications Manager KeepAlive Process

The station, device, or service and the Unified Communications Manager 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 Unified Communications Manager and the station remains active. The following messages can originate from either the Unified Communications Manager 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 Unified Communications Manager and the station is active. Again, these messages can originate from either the Unified Communications Manager or the station.

```
16:03:02.328 CCM|MediaTerminationPointControl - stationOutputKeepAliveAck
tcpHandle=4fa7dc016:03:02.328 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 Unified Communications Manager Intracluster Call Flow Traces

The following SDI traces explore the intracluster call flow in detail. You can identify Cisco Unified IP Phone in the call flow by the directory number (dn), tcpHandle, and IP address. A Cisco Unified IP Phone (dn: 1001,

tcpHandle: 0x4fbbc30, IP address: 172.16.70.231) that is located in Cluster 2 calls another Cisco Unified 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 Unified IP Phone (1001) has gone off hook. The following trace shows the unique messages, TCP handle, and the called number, which display on the Cisco Unified IP Phone. No calling number displays at this point because the user has not tried to dial any digits. The following information displays in the form of Skinny Station messages between the Cisco Unified IP Phones and the Unified Communications Manager.

```
16:05:41.625 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x4fbbc3016:05:41.625 CCM|StationD - stationOutputDisplayText
tcpHandle=0x4fbbc30, Display= 1001
```

The next trace shows Skinny Station messages that go from Unified Communications Manager to a Cisco Unified IP Phone. The first message turns on the lamp on the calling party Cisco Unified IP Phone.

```
16:05:41.625 CCM|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x4fbbc30
```

Unified Communications Manager uses the stationOutputCallState message to notify the station of certain call-related information.

```
16:05:41.625 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
```

Unified Communications Manageruses the stationOutputDisplayPromptStatus message to cause a call-related prompt message to display on the Cisco Unified IP Phone.

```
16:05:41.625 CCM|StationD - stationOutputDisplayPromptStatus tcpHandle=0x4fbbc30
```

Unified Communications Manager 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
```

Unified Communications Manager uses the next message to instruct the Skinny Station about the correct line context for the display.

```
16:05:41.625 CCM|StationD - stationOutputActivateCallPlane tcpHandle=0x4fbbc30
```

The following message indicates that 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 party number. The phone sends StationInit messages, Unified Communications Manager sends StationD messages, and Unified Communications Manager 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 Unified Communications Manager is providing inside dial tone to the calling party Cisco Unified IP Phone.

```
16:05:41.625 CCM|StationD - stationOutputStartTone: 33=InsideDialTone
tcpHandle=0x4fbbc30
```

After Unified Communications Manager detects an incoming message and recognizes that the keypad button **1** has been pressed on the Cisco Unified IP Phone, it immediately stops the output tone.

```
16:05:42.890 CCM|StationInit - InboundStim - KeypadButtonMessageID kpButton: 1
tcpHandle=0x4fbbc3016:05:42.890 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 Unified Communications Manager receives enough digits to match, it provides the digit analysis results in a table format. Unified Communications Manager ignores any extra digits that are pressed on the phone after this point because a match already has been found.

```
16:05:43.562 CCM|Digit analysis: analysis results16:05:43.562
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 Unified Communications Manager 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 Unified Communications Manager is ordering the lamp to blink for incoming call indication on the called party Cisco Unified IP Phone.

```
16:05:43.578 CCM|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampBlink tcpHandle=0x4fbb150
```

In the following traces, Unified Communications Manager provides ringer, display notification, and other call-related information to the called party Cisco Unified IP Phone. Again, you can see that all messages get directed to the same Cisco Unified IP Phone because the same tcpHandle gets used throughout the traces.

```
16:05:43.578 CCM|StationD - stationOutputSetRinger: 2=InsideRing
tcpHandle=0x4fbb15016:05:43.578 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 Unified Communications Manager also provides similar information to the calling party Cisco Unified IP Phone. Again, the tcpHandle differentiates between Cisco Unified IP Phones.

```
16:05:43.578 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=1000,
tcpHandle=0x4fbbc3016:05:43.578 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001,  CallingParty=1001, CalledPartyName=1000, CalledParty=1000,
 tcpHandle=0x4fbbc30
```

In the next trace, Unified Communications Manager provides an alerting or ringing tone to the calling party Cisco Unified IP Phone and provides notification that the connection has been established.

```
16:05:43.578 CCM|StationD - stationOutputStartTone: 36=AlertingTone
tcpHandle=0x4fbbc3016:05:43.578 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 Cisco Unified IP Phone goes off hook; therefore, Unified Communications Manager stops generating the ringer tone to calling party.

```
16:05:45.140 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
```

In the following messages, Unified Communications Manager causes the Skinny Station to begin receiving a Unicast RTP stream. To do so, Unified Communications Manager 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 This value normally gets set to 30 msec. In this case, it gets 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, Unified Communications Manager 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
```

Unified Communications Manager 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 Unified Communications Manager 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 specifies ipAddr, and PortNumber specifies 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
```

Unified Communications Manager uses the following messages to order the station to begin transmitting the audio and video streams to the indicated remote Cisco Unified 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

16:03:25.328 CCM|StationD(1):   TCPPid=[1.100.117.1] OpenMultiReceiveChannel
conferenceID=16777217 passThruPartyID=1000011
compressionType=101(Media_Payload_H263) qualifierIn=?.   myIP: e98e6b80
(128.107.142.233)|<CT::1,100,11,1.1><IP::><DEV::>

16:03:25.375 CCM|StationInit: TCPPid=[1.100.117.1]
StationOpenMultiMediaReceiveChannelAck Status=0, IpAddr=0xe98e6b80, Port=65346,
PartyID=16777233|<CT::1,100,105,1.215><IP::128.107.142.233>

16:03:25.375 CCM|StationD(2):   TCPPid = [1.100.117.2]
star_StationOutputStartMultiMediaTransmission conferenceID=16777218
passThruPartyID=16777250 remoteIpAddress=e98e6b80(66.255.0.0)
remotePortNumber=65346 compressType=101(Media_Payload_H263) qualifierOut=?. myIP:
 e98e6b80 (128.107.142.233)|<CT::1,100,105,1.215><IP::128.107.142.233>
```

In the following traces, the previously explained messages get sent to the called party. The messages that indicate that the RTP media stream 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 finally goes on hook, which terminates all the control messages between the Skinny Station and Unified Communications Manager as well as the RTP stream between Skinny Stations.

```
16:05:46.203 CCM|StationInit - InboundStim - OnHookMessageID tcpHandle=0x4fbbc30
```

Troubleshooting Intercluster Cisco Unified IP Phone Calls

The case study in this section examines a Cisco Unified IP Phone that is calling another Cisco Unified IP Phone that is located in a different cluster. Consider this type of call as an intercluster Cisco Unified IP Phone call.

Related Topics

Call Flow Traces, on page 176
Failed Call Flow, on page 177
Intercluster H.323 Communication, on page 176

Sample Topology, on page 176

Sample Topology

The following sample topology gets used in this case study. Two clusters, each having two Unified Communications Managers, 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 Unified IP Phone in Cluster 2. Intercluster Unified Communications Manager communication takes place by using the H.323 Version 2 protocol. A Cisco IOS Gatekeeper also serves for admission control.

The Cisco Unified IP Phone can connect to the Unified Communications Manager using Skinny Station protocol, and the Unified Communications Manager 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 that the intercluster call can be made by using H.323 version 2 protocol. After this happens, the audio path gets made by using the RTP protocol between Cisco Unified IP Phones in different clusters.

Call Flow Traces

This section discusses the call flow by using SDI trace examples that are captured in the CCM000000000 file. The traces that are discussed in this case study focus only on the call flow itself.

In this call flow, a Cisco Unified IP Phone (2002) that is located in Cluster 2 calls a Cisco Unified 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 Unified IP Phone (2002) went off hook. The trace shows the unique messages, TCP handle, and the calling number, which displays on the Cisco Unified IP Phone. The following debug output shows the called number (1001), H.225 connect, and H.245 confirm messages. The codec type specifies G.711 mu-law.

```
16:06:13.921 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x1c6431016:06:13.953 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 hexidecimal 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 Unified IP Phone (2002). The disconnect, then on-hook messages, follow these traces.

```
RemoteRtpPortNumber: 29626 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k16:06:16.515 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 Unified IP Phone (1001) goes off hook. A TCP handle gets assigned to the Cisco Unified IP Phone.

```
16:05:33.468 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x4fbbc3016:05:33.468 CCM|StationD - stationOutputDisplayText
tcpHandle=0x4fbbc30, Display= 1001
16:05:33.484 CCM|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x4fbbc30
```

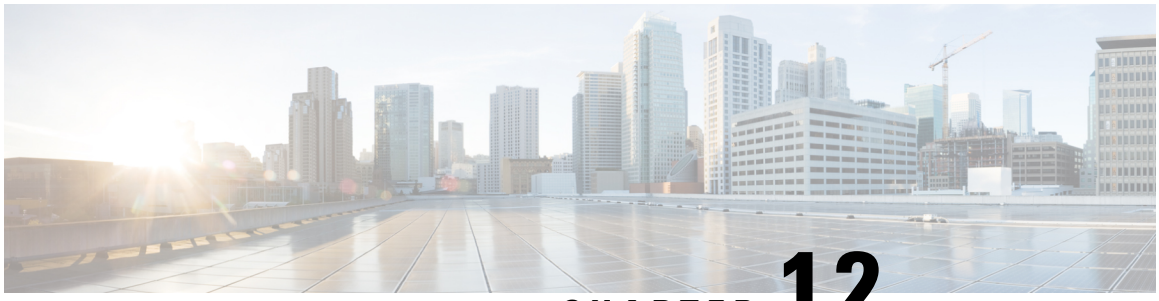
In the following traces, the user dials the called number (2000) of the Cisco Unified IP Phone, and the process of digit analysis tries to match the number.

```
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")
```

Now that the digit analysis is completed, the results display in the following traces. Keep in mind that the following PotentialMatches=NoPotentialMatchesExist reference indicates that the Unified Communications

Manager 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 results16:05:36.812
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
```



CHAPTER 12

Case Study: Troubleshooting Cisco Unified IP Phone-to-Cisco IOS Gateway Calls

This case study examines a Cisco Unified IP Phone that is calling through a Cisco IOS Gateway to a phone that connects 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 that is 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.

- Call Flow Traces, on page 179
- Debug Messages and Show Commands on the Cisco IOS Gatekeeper, on page 182
- Debug Messages and Show Commands on the Cisco IOS Gateway, on page 184
- Cisco IOS Gateway with T1/PRI Interface, on page 187
- Cisco IOS Gateway with T1/CAS Interface, on page 188

Call Flow Traces

This section discusses call flow through examples from the Unified Communications Manager trace file CCM000000000. The traces in this case study focus only on the call flow itself. See topics related to Cisco Unified IP Phone calls for detailed trace information (for example, initialization, registration, and the keepalive mechanism).

In this call flow, a Cisco Unified IP Phone (directory number 1001) that is located in cluster 2 calls 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 Unified IP Phone (1001) went off hook. The trace shows the unique messages, TCP handle, and the calling number, which displays on the Cisco Unified IP Phone Phone. No called number displays at this point, because the user did not try 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 dials 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 Unified Communications Managercurrently active analyzes the digits to discover where the call needs to get routed. See topics related to Cisco Unified IP Phone calls for more details about 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 completed, calling and called party are matched, and the information was 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 gets considered as infinite because the call originated from a Cisco Unified IP Phone that is located in a LAN environment. BW = 64 determines the bandwidth of the destination location. The call destination specifies a phone that is located in a PSTN, and the codec type that is used specifies 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 remain the same because the administrator did not configure 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 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 hexidecimal, and the port numbers.

```
15:20:21.421 CCM|Out Message -- H225SetupMsg -- Protocol= H225Protocol15:20:21.421
 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. The trace also shows is the mapping of a Cisco Unified IP Phone hexidecimal value to the IP address. The IP address of theCisco Unified IP Phone (1001) specifies 172.16.70.231.

```
15:20:21.437 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=3333,
tcpHandle=0x5138d9815:20:21.453 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 get sent, H.323 initializes H.245. The following trace shows the calling and called party information, and the H.245 messages. The TCP handle value remains the same as before, which indicates that this is the continuation of the same call.

```
ONE FOR EACH Channel- 16:53:36.855 CCM|H245Interface(3) paths established ip =
e98e6b80, port = 1304|<CT::1,100,105,1.1682><IP::128.107.142.233>ONE FOR EACH
Channel- 16:53:37.199 CCM|H245Interface(3) OLC outgoing confirm ip = b870701,
port = 49252|<CT::1,100,128,3.9><IP::1.7.135.11>

H323 EP has answered the call and H245 channel setup in progress:
16:53:13.479 CCM|In  Message -- H225ConnectMsg -- Protocol= H225Protocol|

16:03:25.359 CCM|StationD(1):  TCPPid = [1.100.117.1] CallInfo callingPartyName=''
 callingParty=13001 cgpnVoiceMailbox=    calledPartyName='' calledParty=11002
cdpnVoiceMailbox=    originalCalledPartyName='' originalCalledParty=11002
originalCdpnVoiceMailbox= originalCdpnRedirectReason=0
lastRedirectingPartyName='' lastRedirectingParty=11002 lastRedirectingVoiceMailbox=
 lastRedirectingReason=0    callType=2(OutBound) lineInstance=1
callReference=16777217. version: 0|<CT::1,100,11,2.1><IP::><DEV::>

16:03:25.328 CCM|StationD(1):   TCPPid = [1.100.117.1] OpenReceiveChannel
conferenceID=16777217 passThruPartyID=16777233 millisecondPacketSize=20
compressionType=4(Media_Payload_G711Ulaw64k) qualifierIn=?. myIP: e98e6b80
(128.107.142.233)|<CT::1,100,11,1.1><IP::><DEV::>
16:03:25.359 CCM|StationD(2):   TCPPid = [1.100.117.2] StartMediaTransmission
conferenceID=16777218 passThruPartyID=16777249 remoteIpAddress=e98e6b80(64.255.0.0)
    remotePortNumber=65344 milliSecondPacketSize=20
compressType=4(Media_Payload_G711Ulaw64k) qualifierOut=?. myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.213><IP::128.107.142.233>
16:03:25.375 CCM|StationD(2):   TCPPid = [1.100.117.2]
star_StationOutputStartMultiMediaTransmission conferenceID=16777218
passThruPartyID=16777250 remoteIpAddress=e98e6b80(66.255.0.0)
remotePortNumber=65346 compressType=101(Media_Payload_H263) qualifierOut=?. myIP:
 e98e6b80 (128.107.142.233)|<CT::1,100,105,1.215><IP::128.107.142.233>
16:03:25.328 CCM|StationD(1):   TCPPid=[1.100.117.1] OpenMultiReceiveChannel
conferenceID=16777217 passThruPartyID=1000011
compressionType=101(Media_Payload_H263) qualifierIn=?.   myIP: e98e6b80
(128.107.142.233)|<CT::1,100,11,1.1><IP::><DEV::>
```

The following trace shows the H.225 connection message as well as other information. When the H.225 connection message is received, the call connects.

```
15:20:22.968 CCM|In  Message -- H225ConnectMsg -- Protocol=
H225Protocol15:20:22.968 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)
16:03:25.359 CCM|MediaManager(1) - wait_AuConnectInfo - recieved response,
fowarding, CI(16777217,16777218)|<CT::1,100,105,1.213><IP::128.107.142.233>
16:03:25.359 CCM|MediaCoordinator -
wait_AuConnectInfoInd|<CT::1,100,105,1.213><IP::128.107.142.233>
16:03:25.359 CCM|ConnectionManager - wait_AuConnectInfoInd,
CI(16777217,16777218)|<CT::1,100,105,1.213><IP::128.107.142.233>
```

The following message shows that an on-hook message from the Cisco Unified IP Phone (1001) is being received. As soon as an on-hook message is received, the H.225 and Skinny Station device disconnection messages get sent, and the entire H.225 message displays. This final message indicates that the call terminated.

```
15:20:27.296 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x5138d9815:20:27.296 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
16:03:33.344 CCM|StationInit - InboundStim - StationOnHookMessageID: Msg
Size(received, defined) = 4, 12|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|ConnectionManager - wait_AuDisconnectRequest(16777217,16777218):
 STOP SESSION|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2):   TCPPid = [1.100.117.2] CloseReceiveChannel
conferenceID=16777218 passThruPartyID=16777249.  myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2):   TCPPid = [1.100.117.2] StopMediaTransmission
conferenceID=16777218 passThruPartyID=16777249.  myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2):   TCPPid = [1.100.117.2]
star_StationOutputCloseMultiMediaReceiveChannel conferenceID=16777218
passThruPartyID=16777249.  myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2):   TCPPid = [1.100.117.2]
star_StationOutputStopMultiMediaTransmission conferenceID=16777218
passThruPartyID=16777250.  myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.219><IP::128.107.142.233>
```

Related Topics

Case Study: Troubleshooting Cisco Unified IP Phone Calls, on page 167

Debug Messages and Show Commands on the Cisco IOS Gatekeeper

IIn the topology for this case study, the debug ras command turned on in the Cisco IOS Gatekeeper. See topics related to call flow traces for details about SDI trace.

The following debug messages show that the Cisco IOS Gatekeeper is receiving the admission request (ARQ) for the Unified Communications Manager (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 Unified Communications Manager.

```
*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 received a disengage request (DRQ) from the Unified Communications Manager (172.16.70.228), and the Cisco IOS Gatekeeper sent a disengage confirmed (DCF) to the Unified Communications Manager.

```
*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 Unified Communications Managers are registered with the Cisco IOS Gatekeeper. In the topology for this case study, four Unified Communications Managers exist, two in each cluster. This Cisco IOS Gatekeeper includes two zones, and each zone includes two Unified Communications Managers.

R2514-1#show gatekeeper endpoints

```
                    GATEKEEPER ENDPOINT REGISTRATION
=====================================
CallSignalAddr  Port  RASSignalAddr   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
```

Related Topics

Call Flow Traces, on page 179

Debug Messages and Show Commands on the Cisco IOS Gateway

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 Unified Communications Manager (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 TPKT030000650800000100
```

The following debug output shows that the H.225 data is coming from the Unified Communications Manager on this TCP session. The protocolIdentifier, which indicates the H.323 version that is being used, displays 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 specifies 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 uses 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. The peer_tag means dial peer. The calling and called party number in the request packet display.

```
*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 return to the Unified Communications Manager.

```
*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:         },
```

In this packet, Cisco IOS also sends the H.245 address and port number to Unified Communications Manager. 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(0)-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)
```

Related Topics

Debug Messages and Show Commands on the Cisco IOS Gatekeeper..., on page 182

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 got turned on, which enables Q.931, a Layer Three signaling protocol for D-channel in the ISDN environment. Each time that a call is placed out of the T1/PRI interface, a setup packet must get sent. The setup packet always includes (protocol descriptor) pd = 8, and it generates a random hexidecimal 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 represent a 56-Kbps data call and 0x8090A3 if it is a voice call. In the debug following output, the bearer capability specifies 0x8090A3, which applies 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 stays 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 get routed. In this case, a CONNECT message that is received from the switch includes 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 disconnects. A cause ID for the call rejection follows RELEASE_COMP messages. The cause ID represents a hexidecimal value. Find the meaning of the cause by decoding the hexidecimal value and follow 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 was 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
```