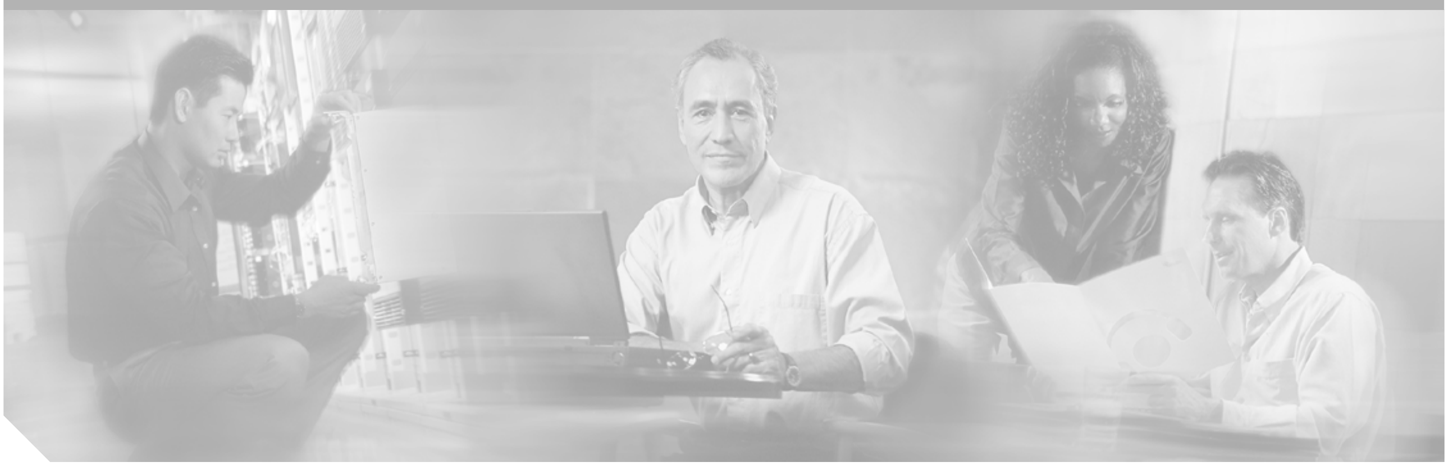


Troubleshooting Guide for Cisco Unified CallManager

Release 5.0(4)

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

Text Part Number: OL-10055-01

CONTENTS

Preface

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

The preface covers these topics:

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

Purpose

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

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

This document does not cover every possible trouble event that might occur on a Cisco Unified CallManager 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 Cisco Unified CallManager* provides guidance for network administrators responsible for managing the Cisco Unified CallManager system, for enterprise managers, and for employees. This guide requires knowledge of telephony and IP networking technology.

Organization

Table 1 shows how this guide is organized.

Table 1 How This Document Is Organized

Chapter and Title	Description
Chapter 1, "Troubleshooting Overview"	Provides an overview of the tools and resources that are available for troubleshooting the Cisco Unified CallManager.
Chapter 2, "Troubleshooting Tools"	Addresses the tools and utilities that you can use to configure, monitor, and troubleshoot Cisco Unified CallManager and provides general guidelines for collecting information to avoid repetitive testing and re-collection of identical data.
Chapter 3, "Cisco Unified CallManager Attendant Console"	Cisco Unified CallManager Attendant Console provides troubleshooting tools for the administrator. These tools include performance counters and alarms that are part of Cisco Unified CallManager Serviceability.
Chapter 3, "Cisco Unified CallManager System Issues"	Describes solutions for the most common issues that relate to a Cisco Unified CallManager system.
Chapter 4, "Device Issues"	Describes solutions for the most common issues that relate to IP phones and gateways.
Chapter 5, "Dial Plans and Routing Issues"	Describes solutions for the most common issues that relate to dial plans, route partitions, and calling search spaces.
Chapter 6, "Cisco Unified CallManager Services Issues"	Describes solutions for the most common issues related to services, such as conference bridges and media termination points.
Chapter 7, "Voice Messaging Issues"	Describes solutions for the most common voice-messaging issues.
Chapter 8, "Troubleshooting Features and Services"	Provides information to help you resolve common issues with Cisco Unified CallManager features and services.
Appendix A, "Opening a Case With TAC"	Describes what information is needed to open a case for TAC.
Appendix B, "Case Study: Troubleshooting Cisco Unified IP Phone Calls"	Describes in detail the call flow between two Cisco Unified IP Phones within a cluster.
Appendix C, "Case Study: Troubleshooting Cisco Unified IP Phone-to-Cisco IOS Gateway Calls"	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 CallManager 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/univercd/cc/td/doc/product/voice/c_callmg/<release #>/doc_gd/index.htm

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

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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

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

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

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.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.

If you require further assistance please contact us by sending email to export@cisco.com.

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

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 on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those 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 using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located 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 are those in which your production network is down or severely degraded.) Cisco TAC engineers are 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

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

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

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

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

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Troubleshooting Overview

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

The section covers following topics:

Cisco Unified CallManager Serviceability

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

- Saves Cisco Unified CallManager services alarms and events for troubleshooting and provides alarm message definitions.
- Saves Cisco Unified CallManager 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 Cisco Unified CallManager cluster through the real-time monitoring tool (RTMT).
- Generates reports for Quality of Service, traffic, and billing information through Cisco Unified CallManager 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 CallManager Serviceability tools.
- Allows Cisco Unified CallManager 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 CallManager Serviceability from the Cisco Unified CallManager Administration window by choosing Cisco Unified CallManager Serviceability from the Navigation drop-down list box. Installing the Cisco Unified CallManager software automatically installs Cisco Unified CallManager Serviceability and makes it available.

Refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System 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 *Cisco Unified Communications Operating System Administration Guide* 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.

Step 1 Analyze the network problem and create a clear problem statement. Define symptoms and potential causes.

Step 2 Gather the facts that you need to help isolate possible causes.

Step 3 Consider possible causes based on the facts that you gathered.

Step 4 Create an action plan based on those causes. Begin with the most likely problem and devise a plan in which you manipulate only one variable.

Step 5 Implement the action plan; perform each step carefully while testing to see whether the symptom disappears.

Step 6 Analyze the results to determine whether the problem has been resolved. If the problem was resolved, consider the process complete.

Step 7 If the problem has not been resolved, create an action plan based on the next most probable cause on your list. Return to Step 4 and repeat the process until the problem 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 Cisco Unified CallManager?
- Do you know all the points of contact to external networks, including any connections to the Internet? For each external network connection, do you know what routing protocol is being used?
- Has your organization documented normal network behavior and performance, so you can compare current problems with a baseline?

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

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, refer to the *Cisco Unified CallManager Documentation Guide*. The following URL shows an example of the path to the documentation guide:

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/<release #>/doc_gd/index.htm
- For documentation related to Cisco Unity, refer to the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.htm l
- For documentation related to Cisco Emergency Responder, refer to the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/respond/index.htm.

- For documentation related to Cisco Unified IP phones, refer to the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm.
- For information on designing and troubleshooting IP telephony networks, refer to the *Cisco IP Telephony Solution Reference Network Design Guides* that are available at www.cisco.com/go/srnd.

Troubleshooting Tools

This section addresses the tools and utilities that you use to configure, monitor, and troubleshoot Cisco Unified CallManager 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.

This section contains the following topics:

Cisco Unified CallManager Serviceability Troubleshooting Tools

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

Table 2-1 Serviceability Tools

Term	Definition
Real-Time Monitoring Tool (RTMT)	This term identifies a program in Serviceability that provides real-time information about Cisco Unified CallManager devices and performance counters as well as enables administrators to collect traces. Performance counters can be system specific or Cisco Unified CallManager specific. Objects comprise the logical groupings of like counters for a specific device or feature, such as Cisco Unified IP Phones or Cisco Unified CallManager 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 run-time status and state of the Cisco Unified CallManager 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 Cisco CallManager service problems. Cisco Unified CallManager Serviceability sends configured trace information to the trace log file. Two types of trace log files exist: SDI and SDL. Every Cisco CallManager 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 CallManager Serviceability.

Command Line Interface

Use the command line interface (CLI) to access the Cisco Unified CallManager 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 Cisco Unified CallManager CLI command set, see the *Cisco Unified Communications Operating System Administration Guide*.

CiscoWorks2000

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

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

Refer to the CiscoWorks2000 documentation for more information on CiscoWorks2000 at the following URL:

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

System Log Management

Although it can be adapted to other network management systems, Cisco Syslog Analysis, which is packaged with CiscoWorks2000 Resource Manager Essentials, 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 Cisco Unified CallManager servers.

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

Cisco Discovery Protocol Support

The Cisco Discovery Protocol Support enables discovery of Cisco Unified CallManager servers and management of those servers by CiscoWorks2000.

Simple Network Management Protocol Support

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

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

- A managed device designates a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

- An agent, as network management software, resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.
- A network management system comprises an SNMP management application together with the computer on which it runs. An NMS executes applications that monitor and control managed devices. An NMS provides the bulk of the processing and memory resources that are required for network management. The following NMSs share compatibility with Cisco Unified CallManager:
  - CiscoWorks2000
  - HP OpenView
  - Third-party applications that support SNMP and Cisco Unified CallManager 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, Cisco Unified CallManagers, 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 `service timestamps debug datetime msec` is globally configured on the gateway.

Note Avoid collecting debugs in a live environment during operation hours.

Preferably, collect debugs during non-working hours. If you must collect debugs in a live environment, configure `no logging console` and `logging buffered`. 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 Cisco Unified CallManager node on your site. Using strong encryption, Cisco Secure Telnet enables a special Telnet client from Cisco Systems to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and troubleshooting of your Cisco Unified CallManager nodes, without requiring firewall modifications.

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

Packet Capture

This section contains information on the following topics:

Packet Capturing Overview

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

- Analyze packets for messages that are exchanged between Cisco Unified CallManager and the device (Cisco Unified IP Phone, Cisco Unified SIP IP Phone, 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 *Cisco Unified CallManager Security Guide*.

Configuration Checklist for Packet Capturing

Extracting and analyzing pertinent data includes performing the following tasks in Table 2-2:

Table 2-2 Configuration Checklist for Packet Capturing

Configuration Steps		Procedures and Topics
Step 1	Add end users to the Standard Packet Sniffer Users group.	Adding an End User to the Standard Packet Sniffer Users Group, page 2-6
Step 2	Configure packet capturing service parameters in the Service Parameter Configuration window in Cisco Unified CallManager Administration; for example, configure the Packet Capture Enable service parameter.	Configuring Packet-Capturing Service Parameters, page 2-7
Step 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.	• Configuring Packet Capturing in the Phone Configuration Window, page 2-7 • Configuring Packet Capturing in Gateway and Trunk Configuration Windows, page 2-8 • Packet-Capturing Configuration Settings, page 2-9
Step 4	Capture SRTP packets by using a sniffer trace between the affected devices.	Refer to the documentation that supports your sniffer trace tool.
Step 5	After you capture the packets, set the Packet Capture Enable service parameter to False.	• Configuring Packet-Capturing Service Parameters, page 2-7 • Packet-Capturing Configuration Settings, page 2-9
Step 6	Gather the files that you need to analyze the packets.	Analyzing Captured Packets, page 2-10
Step 7	Cisco Technical Assistance Center (TAC) analyzes the packets. Contact TAC directly to perform this task.	Analyzing Captured Packets, page 2-10

Adding an End User to the Standard Packet Sniffer Users 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 Users group, the user cannot initiate packet capturing.

The following procedure, which describes how to add an end user to the Standard Packet Sniffer Users group, assumes that you configured the end user in Cisco Unified CallManager Administration, as described in the *Cisco Unified CallManager Administration Guide*.

Procedure

Step 1 Find the user group, as described in the *Cisco Unified CallManager Administration Guide*.

Step 2 After the Find/List window displays, click the **Standard Packet Sniffer Users** link.

Step 3 Click the **Add Users to Group** button.

Step 4 Add the end user, as described in the *Cisco Unified CallManager Administration Guide*.

Step 5 After you add the user, click **Save**.

Configuring Packet-Capturing Service Parameters

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

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System** > **Service Parameters**.

Step 2 From the Server drop-down list box, choose an Active server where you activated the Cisco Unified CallManager service.

Step 3 From the Service drop-down list box, choose the **Cisco CallManager (Active)** service.

Step 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.

Step 5 For the changes to take effect, click **Save**.

Step 6 To continue packet-capturing configuration, see one of the following sections:

- Configuring Packet Capturing in the Phone Configuration Window, page 2-7
- Configuring Packet Capturing in Gateway and Trunk Configuration Windows, page 2-8

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 CallManager Administration.

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

Tip 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

Step 1 Before you configure the packet-capturing settings, see the "Configuration Checklist for Packet Capturing" section on page 2-6.

Step 2 Find the SIP or SCCP phone, as described in the *Cisco Unified CallManager Administration Guide*.

Step 3 After the Phone Configuration window displays, configure the troubleshooting settings, as described in Table 2-3.

Step 4 After you complete the configuration, click **Save**.

Step 5 In the Reset dialog box, click **OK**.

Tip Although Cisco Unified CallManager 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.

See the "Analyzing Captured Packets" section on page 2-10.

Configuring Packet Capturing in Gateway and Trunk Configuration Windows

The following gateways and trunks support packet capturing in Cisco Unified CallManager Administration:

- 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

Step 1 Before you configure the packet-capturing settings, see the "Configuration Checklist for Packet Capturing" section on page 2-6.

Step 2 Perform one of the following tasks:

- Find the Cisco IOS MGCP gateway, as described in the *Cisco Unified CallManager Administration Guide.*
- Find the H.323 gateway, as described in the *Cisco Unified CallManager Administration Guide.*
- Find the H.323/H.245/H.225 trunk, as described in the *Cisco Unified CallManager Administration Guide.*
- Find the SIP trunk, as described in the *Cisco Unified CallManager Administration Guide.*

Step 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 *Cisco Unified CallManager Administration Guide*. 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.

Step 4 Configure the troubleshooting settings, as described in Table 2-3.

Step 5 After you configure the packet-capturing settings, click **Save**.

Step 6 In the Reset dialog box, click **OK**.

Tip Although Cisco Unified CallManager 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.

See the "Analyzing Captured Packets" section on page 2-10.

Packet-Capturing Configuration Settings

Use Table 2-3, which describes the Packet Capture Mode and Packet Capture Duration settings, with the following sections:

- Configuring Packet Capturing in the Phone Configuration Window, page 2-7
- Configuring Packet Capturing in Gateway and Trunk Configuration Windows, page 2-8

Table 2-3 Packet-Capturing Configuration Settings

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, Cisco Unified CallManager sets the Packet Capture Mode to None. • **Batch Processing Mode**—Cisco Unified CallManager 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. Cisco Unified CallManager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CallManager 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.

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 the *Cisco Unified CallManager Security Guide*.

Troubleshooting Perfmon Data Logging

> **Caution** Enabling the troubleshooting perfmon data logging feature impacts system performance on the selected node. Do not enable this parameter unless Cisco Technical Assistance Center (TAC) directs you to do so.

The troubleshooting perfmon data logging feature assists Cisco TAC in identifying system problems. When you enable troubleshooting perfmon data logging, you initiate the collection of a set of Cisco Unified CallManager and operating system performance statistics on the selected node. The statistics that are collected include comprehensive information that can be used for system diagnosis and information from a set of counters that is not a part of the current set of preconfigured counters in the Real-Time Monitoring Tool.

Because an extensive amount of information is collected in a short time, Cisco recommends that you do not enable the troubleshooting perfmon data logging for any extended time and that you enable the Log Partitioning Monitor to monitor disk usage while troubleshooting perfmon data logging is enabled.

When you enable the troubleshooting perfmon data logging feature on a system with no active phone calls and you use the default setting for the troubleshooting perfmon data-logging parameters, Cisco estimates that the system experiences a less than 5-percent increase in CPU utilization and an insignificant increase in the amount of memory that is being used, and it writes approximately 50 MB of information to the log files daily.

You can perform the following administrative tasks with the troubleshooting perfmon data-logging feature:

- Enable and disable the trace filter for Troubleshooting perfmon data logging.
- Monitor a set of predefined System and Cisco Unified CallManager performance objects and counters on each server.
- Log the monitored performance data in CSV file format on the local server in the active log partition in the var/log/active/cm/log/ris/csv directory. The log file uses the following naming convention: PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv; for example, PerfMon_172.19.240.80_06_15_2005_11_25.csv.
- Specify the polling rate. This rate specifies the rate at which performance data gets gathered and logged. You can configure the polling rate down to 5 seconds. Default polling rate equals 15 seconds.
- Specify the maximum number of log files that will be stored on disk. Log files exceeding this limit get purged automatically by removal of the oldest log file. The default specifies 50 files.
- Specify the rollover criteria of the log file based on the maximum size of the file in megabytes. The default value specifies 2 MB.
- Collect the SOAP log file by using the Trace & Log Central feature of the Real-Time Monitoring Tool or Command Line Interface.
- Collect the Cisco RIS Data Collector PerfMonLog log file by using the Trace & Log Central feature of the Real-Time Monitoring Tool or Command Line Interface.
- View the log file in graphical format by using the Microsoft Windows performance tool as described in "Viewing the Perfmon Log Files with the Microsoft Performance Tool" section on page 2-17 or by using the Real-Time Monitoring Tool as described in the *Cisco Unified CallManager Serviceability Administration Guide*.

The troubleshooting perfmon data-logging feature collects information from the following counters within the following perfmon objects. Refer to the “Performance Objects and Counters” chapter in *Cisco Unified CallManager Serviceability System Guide* for a description on the counters:

- Cisco CallManager Object:
  - CallManagerHeartBeat
  - CallsActive
  - CallsAttempted
  - CallsCompleted
  - InitializationState
  - RegisteredHardwarePhones
  - RegisteredMGCPGateway
- Cisco CallManager System Performance Object:
  - AverageExpectedDelay
  - CallsRejectedDueToThrottling
  - QueueSignalsPresent 1-High
  - QueueSignalsPresent 2-Normal
  - QueueSignalsPresent 3-Low
  - QueueSignalsPresent 4-Lowest
  - QueueSignalsProcessed 1-High
  - QueueSignalsProcessed 2-Normal
  - QueueSignalsProcessed 3-Low
  - QueueSignalsProcessed 4-Lowest
  - QueueSignalsProcessed Total
  - TotalCodeYellowEntry
- Cisco TFTP
  - BuildAbortCount
  - BuildCount
  - BuildDeviceCount
  - BuildDialruleCount
  - BuildDuration
  - BuildSignCount
  - BuildSoftkeyCount
  - BuildUnitCount
  - ChangeNotifications
  - DeviceChangeNotifications
  - DialruleChangeNotifications
  - EncryptCount
  - GKFoundCount
  - GKNotFoundCount
  - HeartBeat

- HttpConnectRequests
- HttpRequests
- HttpRequestsAborted
- HttpRequestsNotFound
- HttpRequestsOverflow
- HttpRequestsProcessed
- HttpServedFromDisk
- LDFoundCount
- LDNotFoundCount
- MaxServingCount
- Requests
- RequestsAborted
- RequestsInProgress
- RequestsNotFound
- RequestsOverflow
- RequestsProcessed
- SegmentsAcknowledged
- SegmentsFromDisk
- SegmentsSent
- SEPFoundCount
- SEPNotFoundCount
- SIPFoundCount
- SIPNotFoundCount
- SoftkeyChangeNotifications
- UnitChangeNotifications

- Process Object:
  - PID
  - STime
  - % CPU Time
  - Page Fault Count
  - Process Status
  - VmData
  - VmRSS
  - VmSize
  - Thread Count
- Memory Object:
  - Used Kbytes
  - Free Kbytes
  - Total Kbytes
  - Shared Kbytes

- Buffers Kbytes
- Cached Kbytes
- Free Swap Kbytes
- Total Swap Kbytes
- Used Swap Kbytes
- Pages Input
- Pages Output
- Pages
- Used VM Kbytes
- Total VM Kbytes
- % Page Usage
- % VM Used
- % Mem Used

- Processor Object:
  - Irq Percentage
  - Softirq Percentage
  - IOwait Percentage
  - User Percentage
  - Nice Percentage
  - System Percentage
  - Idle Percentage
  - %CPU Time
- Thread Object—Troubleshooting Perfmon Data Logger only logs CCM threads:
  - %CPU Time
- Partition Object:
  - Used Mbytes
  - Total Mbytes
  - %Used
  - Await Read Time
  - Await Write Time
  - Await Time
  - % CPU Time
  - Read Bytes Per Sec
  - Write Bytes Per Sec
  - Queue Length
- IP Object:
  - In Receives
  - InHdrErrors
  - In UnknownProtos
  - In Discards

  - In Delivers
  - Out Requests
  - Out Discards
  - Reasm Reqds
  - Reasm Oks
  - Reasm Fails
  - Frag OKs
  - Frag Fails
  - Frag Creates
  - InOut Requests
- TCP Object:
  - Active Opens
  - Passive Opens
  - Attempt Fails
  - Estab Resets
  - Curr Estab
  - In Segs
  - Out Segs
  - Retrans Segs
  - InOut Segs
- Network Interface Object:
  - Rx Bytes
  - Rx Packets
  - Rx Errors
  - Rx Dropped
  - Rx Multicast
  - Tx Bytes
  - Tx Packets
  - Tx Errors
  - Tx Dropped
  - Total Bytes
  - Total Packets
  - Tx QueueLen
- System Object:
  - Allocated FDs
  - Freed FDs
  - Being Used FDs
  - Max FDs
  - Total Processes

- Total Threads
- Total CPU Time

The following procedure provides the steps for using the troubleshooting perfmon data- logging feature.

Procedure

Step 1 Configure the Troubleshooting Perfmon Data Logging parameters in the Cisco RIS Data Collector service.

See the"Configuring Troubleshooting Perfmon Data Logging" section on page 2-16

Step 2 Verify that log partition monitoring is enabled.

See the *Cisco Unified CallManager Administration Guide.*

Step 3 Collect the log files for the Cisco RIS Data Collector service on the server that has troubleshooting perfmon data logging enabled

- If you want to download the log files by using RTMT, refer to *Cisco Unified CallManager Serviceability Administration Guide*.
- If you want to download the log files by using the CLI, refer to *Cisco Unified Communications Operating System Administration Guide.*

Step 4 View the log file in graphical format by using the Microsoft Windows performance tool as described in "Viewing the Perfmon Log Files with the Microsoft Performance Tool" section on page 2-17 or by using the Real-Time Monitoring Tool as described in the *Cisco Unified CallManager Serviceability Administration Guide*.

Step 5 When you have collected all the necessary files, disable troubleshooting perfmon data logging by setting the Enable Logging parameter to False.

Configuring Troubleshooting Perfmon Data Logging

The following procedure describes how to configure the troubleshooting perfmon data-logging feature.

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System** > **Service Parameters**.

The Service Parameter Configuration window displays.

Step 2 From the Server drop-down list box, choose the server.

Step 3 From the Service drop-down list box, choose Cisco RIS Data Collector.

Step 4 Enter the appropriate settings as described in Table 2-4.

Step 5 Click **Save.**

Troubleshooting Perfmon Data-Logging Configuration Settings

Table 2-4 describes the available settings to enable and disable troubleshooting perfmon data logging.

Table 2-4 Troubleshooting Perfmon Data-Logging Parameters

Field	Description
Enable Logging	From the drop-down box, choose **True** to enable or **False** to disable troubleshooting perfmon data logging.
Polling Rate	Enter the polling rate interval (in seconds). You can enter a value from 5 (minimum) to 300 (maximum). The default values specifies 15.
Maximum No. of Files	Enter the maximum number of Troubleshooting Perfmon Data Logging files that you want to store on disk. You can enter a value from 1 (minimum) up to 100 (maximum). The default value specifies 50. Consider your storage capacity in configuring the Maximum No. of Files and Maximum File Size Parameters. Cisco recommends that you do not exceed a value of 100 MB when you multiply the Maximum Number of Files value by the Maximum File Size value. When the number of files exceeds the maximum number of files that you specified in this field, Cisco Unified CallManager will delete log files with the oldest timestamp. **Caution** If you do not save the log files on another machine before you change this parameter, you risk losing the log files.
Maximum File Size	Enter the maximum file size (in megabytes) that you want to store in a perfmon log file before a new file is started. You can enter a value from 1 (minimum) to 500 (maximum). The default value specifies 2 MB. Consider your storage capacity in configuring the Maximum No. of Files and Maximum File Size Parameters. Cisco recommends that you do not exceed a value of 100 MB when you multiply the Maximum Number of Files value by the Maximum File Size value.

Viewing the Perfmon Log Files with the Microsoft Performance Tool

To view the log files by using the Microsoft Performance tool, follow these steps:

Procedure

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Performance.**

Step 2 In the application window, click the right mouse button and choose **Properties**.

Step 3 Click the Source tab in the System Monitor Properties dialog box.

Step 4 Browse to the directory where you downloaded the perfmon log file and choose the perfmon csv file. The log file includes the following naming convention: PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv; for example, PerfMon_172.19.240.80_06_15_2005_11_25.csv.

Step 5 Click **Apply.**

Step 6 Click the **Time Range** button. To specify the time range in the perfmon log file that you want to view, drag the bar to the appropriate starting and ending times.

Step 7 To open the Add Counters dialog box, click the Data tab and click **Add**.

Step 8 From the Performance Object drop-down box, choose the perfmon object. If an object has multiple instances, you may choose **All instances** or select only the instances that you are interested in viewing.

Step 9 You can choose **All Counters** or select only the counters that you are interested in viewing.

Step 10 To add the selected counters, click **Add**

Step 11 When you finish selecting counters, click **Close.**

Common Troubleshooting Tasks, Tools, and Commands

This section provides a quick reference for commands and utilities to help you troubleshoot a Cisco Unified CallManager server with root access disabled. Table 2-5 provides a summary of the CLI commands and GUI selections that you can use to gather information troubleshoot various system problems.

Table 2-5 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
Memory	free	RTMT Go to View tab and select Server > CPU and Memory	show perf query class Memory
Network status	netstats		show network status

Table 2-5 Summary of CLI Commands and GUI Selections (continued)

Information	Linux Command	Serviceability GUI Tool	CLI commands
Reboot server	reboot	Log in to Platform Web page on the server Go to Restart > 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

Table 2-6 provides a list of common problems and tools to use to troubleshoot them.

Table 2-6 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 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 Cisco Unified CallManager server after downloading the files to your PC.	file delete

Table 2-6 Troubleshooting Common Problems with CLI Commands and GUI Selections

Task	GUI Tool	CLI commands
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**.	Core [options..]
Rebooting the Cisco Unified CallManager 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 Unified 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 Cisco Unified CallManager.

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

Tip Know where your devices are registered.

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

Verify Cisco Unified CallManager Services Are Running

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

Procedure

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

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

Step 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.

Step 4 Check the check box for the desired Cisco CallManager service.

Step 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

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

The Cisco Unified CallManager Serviceability window displays.

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

Step 3 From the Servers column, choose the server.

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

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

CHAPTER 3

Cisco Unified CallManager System Issues

Updated7-3-2007

This section covers solutions for the following most common issues that relates to a Cisco Unified CallManager system.

Cisco Unified CallManager System Not Responding

This section covers the following issues for a Cisco Unified CallManager system that is not responding:

Cisco Unified CallManager System Stops Responding

Symptom

The Cisco Unified CallManager system does not respond.

When the Cisco CallManager service crashes, 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 the event of a crash follow:

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

The Cisco CallManager 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 Cisco Unified CallManager, users receive delayed dial tone, and/or the Cisco Unified CallManager server freezes due to high CPU usage. For event log messages that are not included here, view the Cisco Unified CallManager Event Logs.

Possible Cause

The Cisco CallManager service can crash 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 crash you experience, you will need to gather different data that will help determine the root cause of the crash.

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

Procedure

Step 1 Collect Cisco CallManager traces 15 minutes before and after the crash.

Step 2 Collect SDL traces 15 minutes before and after the crash.

Step 3 Collect perfmon traces if available.

Step 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 crash.

Cisco Unified CallManager Administration Does Not Display

Symptom

Cisco Unified CallManager 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, as described in "Verify Cisco Unified CallManager Services Are Running" section on page 2-21 or in the *Cisco Unified CallManager Serviceability Administration Guide*.

Error When Attempting to Access Cisco Unified CallManager Administration

Symptom

One of the following messages displays when you are trying to access Cisco Unified CallManager Administration.

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

Possible Cause

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

Recommended Action

Try starting the other services.

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

Symptom

One of the following error messages displays when you are trying to access the Cisco Unified CallManager Administration.

Possible Cause

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

Recommended Action

If this occurs, follow the procedure for changing the IP address on a subsequent Cisco Unified CallManager node in the *Cisco Unified Communications Operating System Administration Guide*.

You Are Not Authorized to View

Symptom

When accessing the Cisco Unified CallManager 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 CallManager

Symptom

You cannot add a user or conduct a search in Cisco Unified CallManager Administration.

Possible Cause

You may encounter the following problems if you are working with Cisco Unified CallManager 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 hit 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 Cisco Unified CallManager Administration, if your Cisco Unified CallManager 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 CallManager 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 CallManager 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 Cisco Unified CallManager 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 Cisco Unified CallManager 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 CallManager 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 Cisco Unified CallManager server, such as ping or Telnet, are allowed. If any are successful, it will show that http access to the Cisco Unified CallManager 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 Cisco Unified CallManager.

When you attempt the same action from other remote machines, Cisco Unified CallManager 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 Cisco Unified CallManager 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 Cisco Unified CallManager network, a routing issue probably exists in the network. Contact the network administrator to verify the routing that is configured in your default gateway.

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

Replication Fails Between the Publisher and the Subscriber

Replicating the database is a core function of Cisco Communications Manager clusters. The server with the master copy of the database is called the publisher, while the servers replicating the database are called subscribers.

Symptom

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

Possible Cause

Replication fails between the publisher and subscriber.

Recommended Action

Complete the following steps to reestablish the relationship between the two systems.

1. Verify the Replication.
   a. Open Cisco Unified Communications Manager Real-Time Monitoring Too (RTMT).
   b. Choose System > Performance > Open Peformance Monitoring.
   c. Double-click the publisher node to expand the performance monitors.
   d. Double-click Replication Counters.
   e. Double-click Number of Replicates Created.
   f. Choose ReplicateCount from the Object Instances dialog box and click Add.
   g. Double-click Replication Status.
   h. Choose ReplicateCount from the Object Instances dialog box and click Add.

Note Right click the counter name and choose Counter Description to view the definition of the counter.

2. Check State of Replication via CLI.
   a. Access the platform CLI and use the following command to check repliaction:

   ```
   utils dbreplication status file view activelog <filename_output_above>
   ```

   b. Review the Summary information and counts for each node to verify replication.

3. To repair replication, use the following procedure:
   a. Access the platform CLI.
   b. Repair replication by using the following command:

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

Slow Server Response

This section addresses a problem that relates to a slow response from the server due to mismatched duplex port settings.

Symptom

Slow response from the server occurs.

Possible Cause

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

Recommended Action

1. For optimal performance, set both switch and server to **100/Full**.

   Cisco does not recommend using the Auto setting on either the switch or the server.

2. You must restart the Cisco Unified CallManager server for this change to take effect.

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 Cisco Unified CallManager and has responsibility for telephony call control. The CRS platform hosts telephony applications, such as Cisco Unified AutoAttendant, 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 CallManager Release Notes for the version of Cisco Unified CallManager that you are using.

To check the version of CRS, log in to the AppAdmin page by typing http://servername/appadmin, where *servername* is the name of the server on which CRS is installed. The current version is located 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

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 appears.

The following list gives the most common errors:

- Unable to create provider—bad login or password
- Unable to create provider—Connection refused
- Unable to create provider—login=
- Unable to create provider—hostname

- Unable to create provider—Operation timed out
- Unable to create provider—null

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-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 -- 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 CMuser page (http://servername/ccmuser) on the Cisco Unified CallManager to ensure that the Cisco Unified CallManager cannot authenticate correctly.

Unable to create provider—Connection refused

Possible Cause

The Cisco Unified CallManager refused the JTAPI connection to the Cisco Unified CallManager.

Full Text of Error Message

```
%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 -- 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 CallManager 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-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 -- 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 Cisco Unified CallManager.

Full Text of Error Message

```
%M%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 -- 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 Cisco Unified CallManager.

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 Cisco Unified CallManager. Make sure no IP routing problems exist. Test connectivity by pinging the Cisco Unified CallManager 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-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 -- 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 Cisco Unified CallManager Plugins window and install it on the CRS server.

MIVR-SS_TEL-1-ModuleRunTimeFailure

Symptom

This exception usually occurs when the JTAPI subsystem is unable to initialize any ports.

Possible Cause

The CRS server can communicate with the Cisco Unified CallManager, but is unable to 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 Cisco Unified CallManager 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 Cisco Unified CallManager configuration and also associates with the JTAPI user on the Cisco Unified CallManager.

Security Issues

This section provides information about security-related measurements and general guidelines for troubleshooting security-related problems. This section contains information on the following topics:

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 CallManager* that matches the model of the phone.

For information about how to delete the CTL file from Cisco Unified IP Phone models 7970, 7960, and 7940 only, see the *Cisco Unified CallManager Security Guide* or the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager* that matches the model of the phone.

Security Alarms

Cisco Unified CallManager Serviceability generates security-related alarms for X.509 name mismatches, authentication errors, and encryption errors. The Serviceability GUI 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 CallManager* 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 Cisco Unified CallManager, the number of authenticated calls that are completed, and the number of authenticated calls that are active at any time. Table 3-1 lists the performance counters that apply to security features.

Table 3-1 Security Performance Counters

Object	Counters
Cisco Unified CallManager	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 *CallManager Serviceability System 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 *Cisco Unified Communications Operating System Administration Guide*.

Reviewing Security Log and Trace Files

Cisco Unified CallManager 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 CallManager 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 *Cisco Unified Communications Operating System Administration Guide*.

Troubleshooting CTL Security Tokens

The section contains information on the following topics:

- Troubleshooting a Locked Security Token After You Consecutively Enter an Incorrect Security Token Password, page 3-15
- Troubleshooting If You Lose One Security Token (Etoken), page 3-16

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

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 *Cisco Unified CallManager Security Guide*. If necessary, purchase new security token(s) to configure the file.

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

Troubleshooting If You Lose One Security Token (Etoken)

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

Procedure

Step 1 Purchase a new security token.

Step 2 Using a token that signed the CTL file, update the CTL file by performing the following tasks:

a. Add the new token to the CTL file.

b. Delete the lost token from the CTL file.

For more information on how to perform these tasks, see the *Cisco Unified CallManager Security Guide*.

Step 3 Reset all phones, as described in the *Cisco Unified CallManager Security Guide*.

Troubleshooting CAPF

This section contains information on the following topics:

- Troubleshooting the Authentication String on the Phone, page 3-16
- Troubleshooting If the Locally Significant Certificate Validation Fails, page 3-17
- Verifying That the CAPF Certificate Installed on All Servers in the Cluster, page 3-17
- Verifying That a Locally Significant Certificate Exists on the Phone, page 3-17
- Verifying That a Manufacture-Installed Certificate (MIC) Exists in the Phone, page 3-17
- CAPF Error Codes, page 3-18

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 Cisco Unified CallManager. If the phone is not registered to the Cisco Unified CallManager, 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 Cisco Unified CallManager, 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 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 on the following topics:

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 CallManager Administration to perform the following tasks if a problem occurs:

- Analyze packets for messages that are exchanged between Cisco Unified CallManager and the device (Cisco Unified IP Phone, Cisco SIP IP Phone, 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 the "Packet Capture" section on page 2-5.

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 Cisco Unified CallManager release, you can configure the packet capture mode for phones. For information about how to perform this task, refer to the *Cisco Unified CallManager Bulk Administration Guide*.

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

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 3-2 CAPF Error Codes

Error Code	Description	Corrective Action
0	CAPF_OP_SUCCESS /*Success */	No correction action required.
1	CAPF_FETCH_SUCCESS_BUT_NO_CERT /* Fetch is successful; however there is no cert */	Install a certificate on the phone. For more information, refer to the *Cisco Unified CallManager Security Guide*.
2	CAPF_OP_FAIL /* Fail */	No corrective action available.
3	CAPF_OP_FAIL_INVALID_AUTH_STR /* Invalid Authentication string */	Enter the correct authentication string on phone. For more information, refer to the *Cisco Unified CallManager Security Guide*.
4	CAPF_OP_FAIL_INVALID_LSC /* Invalid LSC */	Update the locally significant certificate (LSC) on the phone. For more information, refer to the *Cisco Unified CallManager Security Guide*.

Table 3-2 CAPF Error Codes (continued)

Error Code	Description	Corrective Action
5	CAPF_OP_FAIL_INVALID_MIC, /* Invalid MIC */	The manufacture-installed certificate (MIC) has been invalidated. You must install a LSC. For more information, refer to the *Cisco Unified CallManager Security Guide*.
6	CAPF_OP_FAIL_INVALID_CRENDENTIALS, /* Invalid credential */	Enter correct credentials.
7	CAPF_OP_FAIL_PHONE_COMM_ERROR, /* Phone Communication Failure*/	No corrective action available.
8	CAPF_OP_FAIL_OP_TIMED_OUT, /* Operation timeout */	Reschedule the operation.
11	CAPF_OP_FAIL_LATE_REQUEST /* User Initiated Request Late */	Reschedule the CAPF operation.

CHAPTER 4

Device Issues

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

Voice Quality

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

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

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

- Gateways
- Phones
- Networks

This section covers the following common voice-quality problems:

Lost or Distorted Audio

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 Cisco Unified CallManager 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 CallManager 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 *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide* 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 CallManager 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 as described in the "Lost or Distorted Audio" section on page 4-2; 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.

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 (in other words, does not have the global configuration command **no ip routing**).

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

voice-ios-gwy(config)#ip routing

Check Basic IP Routing

Basic IP reachability should always be checked first. As RTP streams are connectionless (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 7910—Press the Settings button, select option 6, push volume down until the Default Router field shows up.
- Cisco Unified IP Phone model 7960/40—Press Settings button, select option 3, scroll down until the Default Router field shows up.
- Cisco Unified IP Phone model 2SP+/30VIP—Press ****#**; then, press **#** until gtwy= 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 Cisco Unified CallManager 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 Cisco Unified CallManager 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 *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
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 *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XXrrrrrXrXrXrXrXrXrXrXrXrXrXrXrrXXrrXrXrXrXrXrXXXXXXXXXXXXXXXrXXXXXXXXXrXrXrXXrrXr
XrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr

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

*Mar 3 23:53:30.378: ****** cut through in BOTH direction *****
```

```
XRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXR
XXRRXRXRXXRRXRXRXRXRXXRXRXRXRXRRXRXXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRXXRXRXRXRXRXRXRXRRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XXRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
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 Unified IP Phone SP12 series and VIP 30—G.711a-law/mu-law, G.723.1
> Cisco Access Gateway DE30 and DT-24+—G.711a-law/mu-law, G.723.1

Location and Bandwidth

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

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

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

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

Phone Issues

This section addresses the following phone issues:

- Phone Resets
- Dropped Calls

Phone Resets

Symptom

Phone resets.

Possible Cause

Phones will power cycle or reset for two reasons:

- TCP failure connecting to Cisco Unified CallManager
- 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 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 (such as Cisco Unified IP Phone model 7960 or Cisco Unified IP Phone model 30VIP) 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 (see the "Phone Resets" section on page 4-10) 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 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 Cisco Unified CallManager alive, so the Cisco Unified CallManager resets the connection. This may occur because a phone was turned off, or a problem may exist in the network. If this is an intermittent problem, you may find it useful to use Performance Monitoring in RTMT.
3. If the problem seems to be occurring only through a certain gateway, such as a Cisco Access DT-24+, enable tracing and/or view the Call Detail Records (CDR). The CDR files will give a cause of termination (CoT) that may help determine the cause of the problem. Refer to the *Cisco Unified CallManager 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/univercd/cc/td/doc/product/software/ios113ed/dbook/disdn.htm.
5. If the call is going out of a gateway to the PSTN, you can use the CDR to determine which side is hanging up the call. Obtain much of the same information by enabling tracing on the Cisco Unified CallManager. Because the trace tool can affect Cisco Unified CallManager performance, you will want to use this option only as a last resort or if your network is not yet in production.

Gateway Issues

This section addresses the following gateway issues:

- Gateway Reorder Tone
- Gateway Registration Failure

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 Cisco Unified CallManager 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 Cisco Unified CallManager.

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 via 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 por*t

    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 via DNS. If successful, the CiscoCM1 IP address will take precedence over anything that the DHCP server or NMP tells it for the TFTP server address, even if the NMP has DHCP disabled.

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

```
TaskID: 0
Cmd:    show 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: 6
Cmd:     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 Cisco Unified CallManager:

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

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

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

22. Check the TFTP trace on the Cisco Unified CallManager.

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

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

The following example shows what the tracy output would look like if the gateway is
not in the Cisco CallManager database:
00:00:01.670 (CFG) Booting DHCP for dynamic configuration.
00:00:05.370 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT_REBOOT
00:00:05.370 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.370 (CFG) Requesting DNS Resolution of CiscoCM1
00:00:05.370 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.370 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.370 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP Server
00:00:05.370 (CFG) TFTP Error: .cnf File Not Found!
00:00:05.370 (CFG) Requesting SAADefault.cnf File From TFTP Server
00:00:05.380 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.380 (CFG) Updating Configuration ROM...
00:00:05.610 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.610 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:05.610 GMSG: Attempting TCP socket with CCM 10.123.9.2
```

```
00:00:05.610 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = 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 CCM 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 = SentRegister
00:00:08.010 GMSG: TFTP Request for application load A0021300
00:00:08.010 GMSG: CCM#0 CPEvent = LOADID --> CPState = AppLoadRequest
00:00:08.010 GMSG: ***TFTP Error: File Not Found***
00:00:08.010 GMSG: CCM#0 CPEvent = LOAD_UPDATE --> CPState = LoadResponse
```

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

```
ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE
00:00:00.050 NMPTask:got message from XA Task
00:00:00.050 (NMP) Open TCP Connection ip:7f010101
00:00:00.050 NMPTask:Send Module Slot Info
00:00:00.060 NMPTask:get DIAGCMD
00:00:00.160 (DSP) Test Begin -> Mask<0x00FFFFFF>
00:00:01.260 (DSP) Test Complete -> Results<0x00FFFFFF/0x00FFFFFF>
00:00:01.260 NMPTask:get VLANCONFIG
00:00:02.030 (CFG) Starting DHCP
00:00:02.030 (CFG) Booting DHCP for dynamic configuration.
00:00:05.730 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT_REBOOT
00:00:05.730 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.730 (CFG) Requesting DNS Resolution of CiscoCM1
00:00:05.730 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.730 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.730 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP Server
00:00:05.730 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.730 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.730 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:05.730 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:05.730 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = 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 CCM 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 Cisco Unified CallManager Administration.

Gatekeeper Issues

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

- Admission Rejects, page 4-17
- Registration Rejects, page 4-17

Admission Rejects

Symptom

The system issues Admission Rejects (ARJ) when Cisco Unified CallManager 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 Cisco Unified CallManager 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 Cisco Unified CallManager is in the allowed subnets.
4. Verify that the technology prefix matches between the Cisco Unified CallManager and the gatekeeper configuration.
5. Verify the bandwidth configuration.

Registration Rejects

Symptom

The system issues Registration Rejects (RRJ) when Cisco Unified CallManager 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 Cisco Unified CallManager 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 Cisco Unified CallManager system receives a Release Complete with cause ie=channel not available, the system sends out a Restart to bring this channel back to the idle state.

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 Cisco Unified CallManager server, the Cisco Unified CallManager releases any call requests for this channel.

This behavior occurs on numerous sites in the UK and when the gateway is an E1 blade (most likely the same happens when 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.

Dial Plans and Routing Issues

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

- Route Partitions and Calling Search Spaces
- Group Pickup Configuration
- Dial Plan Issues

Route Partitions and Calling Search Spaces

Route partitions inherit the error-handling capabilities for the Cisco Unified CallManager 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 *Cisco Unified CallManager Administration Guide* and the *Cisco Unified CallManager System Guide* for more information.

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

```
08:38:54.968 CCM CallManager|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x6b88028
08:38:54.968 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=PotentialMatchesExist
```

```
08:38:54.968 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 Cisco Unified CallManager 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=0x6b88028
08:38:58.734 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 the following dial plan issues:

- Problem When Dialing a Number
- Secure Dial Plan

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 Cisco Unified CallManager 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 *Cisco Unified CallManager Administration Guide* 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, Cisco Unified CallManager 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 Cisco Unified CallManager Administration and use it to examine all the route patterns for the partitions that are in the Calling Search Space for the problem call.
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 Cisco Unified CallManager.
12. If a gateway has no access to Cisco Unified CallManager, 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 Cisco Unified CallManager to create a secure dialing plan for users. Partitions and Calling Search Spaces provide an integral part of security and are especially useful for multitenant environments and for creating an individual user level. Filtering, a subset of the Calling Search Space/Partition concept, can add additional granularity to the security plan.

Be advised that usually the last thing 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.

Cisco Unified CallManager Services Issues

This section covers the solutions for the following most common issues that relate to Cisco Unified CallManager services:

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 Cisco Unified CallManager.
2. Use the Cisco Unified CallManager 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 Cisco Unified CallManager releases. Refer to the appropriate version of Cisco Unified CallManager documentation at the following location: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

```
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 Cisco Unified CallManager.

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

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

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

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

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

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

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.

Hardware Transcoder Not Working As Expected

Symptom

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

Possible Cause

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

Recommended Action

Use the Cisco Unified CallManager 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 Cisco Unified CallManager releases. Refer to the appropriate version of Cisco Unified CallManager documentation at the following location: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

```
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 Cisco Unified CallManager.

```
greece-sup (enable) sh port 4/2
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ----------
 4/2                     enabled    1            full     - MTP

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 4/2     disable 00-10-7b-00-0f-b1 10.200.72.32    255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- -----------
 4/2     10.200.72.25      -               10.200.72.25    -

Port     DNS-Server(s)     Domain
-------- ----------------- -------------------------------------------
 4/2     -                 0.0.0.0

Port     CallManagerState DSP-Type
-------- ---------------- --------
 4/2     registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 4/2  disabled   disabled
```

Note You cannot configure the same E1 port for both Conference Bridge and Transcoder/MTP

To make a call between two devices that are using a low bit rate code (such as G.729 and G.723) that do not support the same codec, you need a transcoder resource.

Assume Cisco Unified CallManager has been configured such that the codec between Region1 and Region2 is G.729. The following scenarios apply:

- If caller on Phone A initiates a call, Cisco Unified CallManager realizes it is a Cisco Unified IP Phone model 7960, which supports G.729. After the digits are collected, the Cisco Unified CallManager determines that the call is destined for User D who is in Region2. Because the destination device also supports G.729, the call gets set up, and the audio flows directly between Phone A and Phone D.
- If a caller on Phone B, who has a Cisco Unified IP Phone model 12SP+, initiates a call to Phone D, this time the Cisco Unified CallManager would realize that the originating phone only supports G.723 or G.711. Cisco Unified CallManager would need to allocate a transcoding resource so audio

would flow as G.711 between Phone B and the transcoder but as G.729 between the transcoder and Phone D. If no transcoder were available, Phone D would ring, but as soon as the call was answered, the call would disconnect.

- If a user on Phone B calls Phone F, which is a Cisco Unified IP Phone model 12SP+, the two phones would actually use G.723, even though G.729 is configured as the codec to use between the regions. G.723 gets used because both endpoints support it, and it uses less bandwidth than G.729.

No Supplementary Services 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 Cisco Unified CallManager.
2. Use Performance monitoring in the Cisco Unified CallManager 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 Cisco Unified CallManager releases. Refer to the appropriate version of Cisco Unified CallManager documentation at the following location: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

```
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 Cisco Unified CallManager.

```
greece-sup (enable) sh port 4/2
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ----------
 4/2                     enabled    1            full     - MTP

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 4/2     disable 00-10-7b-00-0f-b1 10.200.72.32    255.255.255.0
```

```
Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- -----------
 4/2     10.200.72.25      -               10.200.72.25    -

Port     DNS-Server(s)     Domain
-------- ----------------- -------------------------------------------
 4/2     -                 0.0.0.0

Port     CallManagerState DSP-Type
-------- ---------------- --------
 4/2     registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 4/2  disabled   disabled
```

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

Voice Messaging Issues

This section covers the solutions for the following 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, 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

Symptom

When Cisco Unity is running with Cisco Unified CallManager, a caller has 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 CallManager 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.html3.

Cisco Unity Does Not Roll Over: Receive Busy Tone

Symptom

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

Example

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

Possible Cause

The Cisco Messaging Interface (CMI) service is configured with the same number as Cisco Unity (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 Forwarded to Voice Messaging System Are Treated as a Direct Call to Cisco Unity

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 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 systems that are using Cisco Unified CallManager.

Recommended Action

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

Administrator Account Not Associated with Cisco Unity Subscriber

Symptom

While attempting to access the System Administrator (SA) page, you receive a message stating that the administrator account is not associated with the 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, refer to *Granting Administrative Rights to Other Cisco Unity Servers at the following URL:* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity31/sag/sag312/sag_0255.htm#xtocid8

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 appendix provides information to help you resolve common issues with Cisco Unified CallManager features and services:

Troubleshooting Cisco Extension Mobility

Cisco Extension Mobility provides troubleshooting tools for the administrator. These tools include performance counters and alarms that are part of Cisco Unified CallManager Serviceability. For information about performance counters and alarms, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

This section provides the following information to help you troubleshoot problems with Cisco CallManager Extension Mobility:

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 CallManager Serviceability, choose **Trace** > **Trace Configuration**
  - From the Servers drop-down list box, choose a server.
  - Choose **Cisco Extension Mobility** from the drop-down menu of Configured Services.

- 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 Table 8-1.

Table 8-1 Troubleshooting Cisco Unified CallManager 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 Table 8-2 to troubleshoot the error codes and error messages that display on the phone when Cisco Extension Mobility is used.

Table 8-2 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 *Cisco Unified CallManager Features and Services Guide*.
205	[205]-User Profile Absent	Make sure that you have associated a Device Profile to the user. *Cisco Unfed CallManager Features and Services Guide*.
208	[208]-EMService Conn. error	Verify that the Cisco Extension Mobility service is running by choosing **Cisco Unified CallManager Serviceability > Tools > Control Center—Feature Services**.

Table 8-2 Troubleshooting Error Messages That Display on the Phone (continued)

Error Code	Message on Phone	Recommended Action
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 CallManager Serviceability > Tools > Control Center—Network Services**.
	Http Error [503]	If you get this error when Services button is pressed, then check that the Cisco CallManager Cisco IP Phone Services service is running by choosing **Cisco Unified CallManager Serviceability > Tools > Control Center—Feature Services**. If you get this error when you select Extension Mobility service, then check that the Cisco Extension Mobility Application service is running by choosing **Cisco Unified CallManager 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 Cisco Unified CallManager 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.
207	[207]-Device Name Empty	Check that the URL that is configured for Cisco Extension Mobility is correct.

Troubleshooting Cisco Unified CallManager Assistant

This section covers solutions for the most common issues that relate to Cisco Unified CallManager Assistant. Table 8-3 describes troubleshooting tools for Cisco Unified CallManager Assistant and the client desktop.

Table 8-3 Cisco Unified CallManager Assistant Troubleshooting Tools and Client Desktop

Tool Description	Location
Cisco Unified CM 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 Cisco Unified CallManager Real-Time Monitoring Tool (RTMT). Refer to the *Cisco Unified CallManager Serviceability Administration* Guide for more information. You can enable debug tracing by choosing **Cisco Unified CallManager Serviceability** > **Trace** > **Configuration**.
Cisco IPMA client trace files	$INSTALL_DIR\logs\ACLog*.txt on the client desktop in the same location where the Cisco Unified CallManager 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 Cisco Unified CallManager Assistant assistant console resides.
Cisco IPMA Client AutoUpdater trace files	$INSTALL_DIR\UpdatedLog.txt on the client desktop in the same location where the Cisco Unified CallManager Assistant assistant console resides.
Install directory	By default—C:\Program Files\Cisco\Unified CallManager Assistant Console\

The following sections describe Cisco Unified CallManager Assistant error and recovery procedures:

- IPMAConsoleInstall.jsp Displays Error: HTTP Status 503—This Application is Not Currently Available, page 8-5
- IPMAConsoleInstall.jsp Displays Error: No Page Found Error, page 8-5
- Exception: java.lang.ClassNotFoundException: InstallerApplet.class, page 8-6
- Automatic Installation of MS Virtual Machine Is No Longer Provided for Download, page 8-6
- User Authentication Fails, page 8-7
- Assistant Console Displays Error: System Error - Contact System Administrator, page 8-7
- Assistant Console Displays Error: Cisco IP Manager Assistant Service Unreachable, page 8-8
- Calls Do Not Get Routed When Filtering Is On Or Off, page 8-9
- Cisco IP Manager Assistant Service Cannot Initialize, page 8-10

- Calling Party Gets a Reorder Tone, page 8-10
- Manager Is Logged Out While the Service Is Still Running, page 8-10
- Manager Cannot Intercept Calls That Are Ringing on the Assistant Proxy Line, page 8-11
- Not Able to Call the Manager Phone When Cisco IP Manager Assistant Service is Down, page 8-11

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

Probable 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 CallManager Serviceability > Tools > Service Activation**.

If the Cisco IP Manager Assistant service has been activated, restart the Cisco Unified CallManager Assistant by choosing **Cisco Unified CallManager 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

Probable Cause #1

Network problems. For more information on system issues, refer to the "Cisco Unified CallManager System Issues" section on page 3-1.

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.

Probable Cause #2

Misspelled URL.

Corrective Action #2

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

Exception: java.lang.ClassNotFoundException: InstallerApplet.class

Symptom

The Assistant Console fails to install from the web. The following error message displays:

Exception: java.lang.ClassNotFoundException: InstallerApplet.class

Probable Cause

Using the Sun Java plugin virtual machine instead of the Microsoft JVM with the standard Cisco Unified CallManager 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 plugin: 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

Probable 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 plugin for IE from the following URL:

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

  When the Sun Java plugin 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 screen from the assistant console.

Probable 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 Cisco Unified CallManager user through Cisco Unified CallManager Administration.

You must administer the user as an assistant or a manager by associating the Cisco Unified CallManager Assistant user information, which you access through **Cisco Unified CallManager 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

Probable Cause #1

You may have upgraded the Cisco Unified CallManager 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 > Cisco Unified CallManager Assistant > Uninstall Assistant Console** and reinstall the console from URL https://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp.

Probable Cause #2

The user was not configured correctly in the database.

Corrective Action #2

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

You must administer the user as an assistant or a manager by associating the Cisco Unified CallManager Assistant user information, which you access through **Cisco Unified CallManager Administration > User Management > End User**. For more information, see the *Cisco Unified CallManager Features and Services Guide*.

Probable Cause #3

When you deleted a manager from an assistant, Cisco Unified CallManager Administration left a blank line for the assistant

Corrective Action #3

From the Assistant Configuration window, reassign the proxy lines. For more information, see the *Cisco Unified CallManager Features and Services Guide*.

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 be stopped.

Corrective Action #1

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

Probable Cause #2

The server address for the Primary and Secondary Cisco Unified CallManager 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

Step 1 Choose **Cisco Unified CallManager Administration** > **System** > **Server.**

Step 2 Replace the DNS name of the server with the corresponding IP address.

Step 3 Restart the Cisco Unified CallManager Assistant by choosing **Cisco Unified CallManager Serviceability** > **Tools** > **Control Center—Feature Services**.

Probable Cause #3

The Cisco CTI Manager service may be stopped.

Corrective Action #3

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

Probable Cause #4

The Cisco Unified CallManager 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 error message displays in the alarm viewer or in the Cisco Unified CallManager 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 the *Cisco Unified CallManager Features and Services Guide*.

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

Calls Do Not Get Routed When Filtering Is On Or Off

Symptom

Calls do not get routed properly.

Probable Cause #1

Cisco CTI Manager service may be stopped.

Corrective Action #1

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

Probable Cause #2

The Cisco Unified CallManager Assistant route point is not configured properly.

Corrective Action #2

Use wild cards to match the directory number of the Cisco Unified CallManager Assistant CTI route point and the primary directory numbers of all managers configured for Cisco Unified CallManager Assistant.

Probable Cause #3

The status window on the manager phone displays the message, Filtering Down.
Cisco Unified CallManager 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

Step 1 From Cisco Unified CallManager Administration, choose **Device** > **CTI Route Point**.

Step 2 Find the route point, or add a new route point. See the *Cisco Unified CallManager Administration Guide* for configuration details.

Step 3 Restart the Cisco IP Manager Assistant services by choosing **Cisco Unified CallManager 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.

Probable Cause

The Cisco IP Manager Assistant service cannot open a connection to CTIManager. The error message can be seen in the alarm viewer or in the Cisco Unified CM Assistant service logs.

Corrective Action

Restart the Cisco CTI Manager and Cisco IP Manager Assistant services by choosing **Cisco Unified CallManager 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."

Probable 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 *Cisco Unified CallManager Administration Guide*.

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

Probable Cause

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

Corrective Action

The Cisco Unified CallManager administrator must update the manager configuration. Perform the following procedure to correct the problem.

Procedure

Step 1 From Cisco Unified CallManager Administration, choose **User Management > End User**.

The Find and List Users window displays.

Step 2 Enter the manager name in the search field and click the **Find** button.

Step 3 Choose the manager from the results list that you want to update.

The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose **Cisco IPMA Manager** and click **Go**.

Step 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.

Probable Cause

The calling search space of the proxy line is improperly configured.

Corrective Action

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

Procedure

Step 1 From Cisco Unified CallManager Administration, choose **Device > Phone**.

The Find and List Phones search window displays.

Step 2 Click the assistant phone.

The Phone Configuration window displays.

Step 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.

Probable Cause

The Cisco Unified CallManager Assistant CTI route point is not enabled for Call Forward No Answer.

Corrective Action

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

Procedure

Step 1 From Cisco Unified CallManager Administration, choose **Device** > **CTI Route Point**.

The Find and List CTI Route Point search window displays.

Step 2 Click the **Find** button.

A list of configured CTI Route Points display.

Step 3 Choose the Cisco Unified CallManager Assistant CTI route point that you want to update.

Step 4 In the CTI Route Point Configuration window, click the line to update from the Directory Numbers b ox.

The Directory Number Configuration window displays.

Step 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).

Step 6 In the Calling Search Space drop-down list box, choose CSS-M-E (or appropriate calling search space).

Step 7 Click the **Update** button.

Troubleshooting Cisco Unified CallManager Attendant Console

Cisco Unified CallManager Attendant Console provides troubleshooting tools for the administrator. These tools include performance counters and alarms that are part of Cisco Unified CallManager Serviceability. For more information about performance counters and alarms, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

This section provides the following information to help you troubleshoot problems with Cisco Unified CallManager Attendant Console:

- Initialization of Telephony Errors, page 8-13
- Problems Making and Receiving Calls, page 8-15
- Directory Issues, page 8-17
- Voice-Messaging Issues, page 8-18
- Problems Using Cisco Unified CallManager Attendant Console Interface, page 8-18
- Cisco Unified CallManager Serviceability Does Not Generate JTAPI Logs, page 8-20
- Collecting Server Logs, page 8-21
- Performance Monitor Counters for Cisco Unified CallManager Attendant Console, page 8-22

Initialization of Telephony Errors

This section addresses the following Cisco Unified CallManager Attendant Console telephone initialization error message displays:

- Initialization of Telephony Fails, page 8-13
- Initialization of Call Control Fails, page 8-14
- Attendant Cannot Access Server Error Message Displays, page 8-15

Initialization of Telephony Fails

Symptom

The attendant received a message that the initialization of telephony failed.

Possible Cause

The following list gives additional causes:

- No attendant console application user and/or authorization user exists.
- The controlled phones do not reside in the controlled device list of the attendant console authorization user.
- The user names that you set for the attendant console application user and the authorization user on the Application Configuration window do not match the usernames that you set for these users in the Cisco CallManager Attendant Console Server service parameters.
- The attendant console application user is not associated to the Standard CTI Enabled user group, Standard CTI Allow Call Park Monitoring user group, and/or the Standard Allow Control of All Devices user group in Cisco Unified CallManager Administration.

Recommended Action

Make sure that you perform the following tasks:

- Create the attendant console application user and authorization user as described in the *Cisco Unified CallManager Features and Services Guide*.
- Enter the same usernames for the attendant console application user and the authorization user on the Application Configuration window as you do in the Cisco CallManager Attendant Console Server service parameters.
- Make sure that the user ID that you use for the attendant console application user is the same as the value in the JTAPI username field in the Service Parameters Configuration window for the Cisco CallManager Attendant Console Server service.
- Make sure that the user ID that you use for the attendant console authorization user is the same as the value in the ACDeviceAuthorization username field in the Service Parameters Configuration window for the Cisco CallManager Attendant Console Server service.
- Associate the attendant console application user to the Standard CTI Enabled user group, Standard CTI Allow Call Park Monitoring user group, and the Standard Allow Control of All Devices user group in Cisco Unified CallManager Administration as described in the *Cisco Unified CallManager Features and Services Guide*.

Initialization of Call Control Fails

Symptom

The Cisco Unified CallManager Attendant Console failed to initialize call control.

Possible Cause

Call control does not come up for one of two reasons:

- You installed Windows XP SP2 on the attendant PC, and you did not unblock the firewall.
- You unchecked the Allow Control of Device from CTI check box on the Phone Configuration window for the attendant phone.

Recommended Action

Perform one of the following actions:

- Make sure that you check the Allow Control of Device from CTI check box on the Phone Configuration window for each attendant phone. The system enables this field by default. If this check box is not checked for the attendant phone, call control does not come up for the attendant console.
- When you start Cisco Unified CallManager Attendant Console for the first time after you install Windows XP SP2, a dialog box displays that indicates that Windows Firewall blocked some features of the ACClient application. To create an exception in the Windows Firewall, so you can continue using Cisco Unified CallManager Attendant Console, click **Unblock**. The operating system configures the exception automatically.

  If you do not click Unblock when you open Cisco Unified CallManager Attendant Console for the first time after you install Windows XP SP2, use the following procedure to create an exception, so you can continue using Cisco Unified CallManager Attendant Console:

Procedure

Step 1 Choose **Start > Settings > Control Panel > Windows Firewall**.

The Windows Firewall dialog box displays.

Step 2 Choose the Exceptions tab.

Step 3 Click the **Add Program** button.

The Add a Program dialog box displays.

Step 4 Click **Browse**. Navigate to the ACClient.exe file and click **Open**.

The ACClient displays in the application list on the Exceptions tab of the Windows Firewall dialog box.

Step 5 Click **Edit**.

The Edit a Program dialog box displays.

Step 6 Click **Change Scope**.

The Change Scope dialog box displays.

Step 7 Make sure that you choose the **Any computer (including those on the internet)** radio button.

Step 8 Click **OK** twice.

Attendant Cannot Access Server Error Message Displays

Symptom

When the attendant attempted to log in to the server, a dialog box stated that the attendant cannot access the server.

Possible Cause

The version of the attendant console that is on the attendant PC and the version of the attendant console that is available through Cisco Unified CallManager Administration do not match.

Recommended Action

Upgrade the version of the attendant console that is running on the attendant PC. To access the plugin from Cisco Unified CallManager Administration, choose **Application** > **Plugins**. After you install the application, you can configure or update any attendant console settings that you did not configure during the installation process.

Problems Making and Receiving Calls

This section addresses the following Cisco Unified CallManager Attendant Console issues that relate to problems when calls are made or received:

- Unable to Place Calls to Pilot Point, page 8-15
- Line Not Available, page 8-16
- Lines Disabled on Phone, page 8-16

Unable to Place Calls to Pilot Point

Symptom

When a user calls the pilot point, the user gets a reorder tone.

Possible Cause

The controlled device list of the attendant console authorization user does not include the controlled phones.

Recommended Action

You must configure one attendant console authorization user in Cisco Unified CallManager Administration and associate the attendant phones with the user. If you do not configure this user, the attendant console cannot interact with CTIManager, and the attendant cannot receive calls. For more details on creating the authorization user, refer to the *Cisco Unified CallManager Features and Services Guide*.

Line Not Available

Symptom

The attendant received a message that the selected line is not available.

Possible Cause

The line supports a configurable number of calls at the same time. If the attendant line supports two calls and you use Line 1 for transferring a call, and attendant placed another call on hold on the same line, the line that the attendant chose will be unavailable for use. The line remains unavailable until the attendant completes one of the tasks.

Recommended Action

To increase the number of calls supported by a line, perform the following procedure:

Procedure

Step 1 Choose **Device > Phone**.

The Find and List Phones window displays.

Step 2 Enter search criteria to locate a specific phone.

A list of phones that match the search criteria displays.

Step 3 Click the name of the phone to update.

The Phone Configuration window displays.

Step 4 From the Directory Numbers list, click the line that you want to update.

The Directory Number Configuration window displays.

Step 5 In the Maximum Number of Calls field, enter the number of calls that you want the line to support.

Step 6 Click **Update**.

Step 7 For the changes to take effect, click **Reset Devices**.

A message indicates the number of devices that you want to restart.

Step 8 To restart the devices, click **OK**.

Lines Disabled on Phone

Symptom

The lines on the attendant phone are disabled in Cisco Unified CallManager Attendant Console.

Possible Cause

The controlled phones do not appear in the controlled device list of the attendant console authorization user.

Recommended Action

Create an attendant console authorization user and associate the attendant phones with this user as described in the *Cisco Unified CallManager Features and Services Guide*.

Directory Issues

This section addresses the issue of the Directory window not displaying users and provides various probable causes and corrective actions:

Symptom

Users that were added in Cisco Unified CallManager Administration do not appear in the Directory window of Cisco Unified CallManager Attendant Console.

Possible Cause

The server only extracts the user list from the directory when one of the following conditions occurs:

- The Cisco CallManager Attendant Console Server service starts, and the Directory Sync Period service parameter specifies a non-zero interval.
- The interval specified in the Directory Sync Period service parameter expires.
- You change the value of the Directory Sync Period service parameter in Cisco Unified CallManager Administration.

The Cisco Unified CallManager Attendant Console loads the user list only at login.

Recommended Action

The attendant needs to log in again after any of the previous conditions occurs.

Possible Cause

Cisco Unified CallManager Attendant Console does not display users without telephone numbers.

Recommended Action

Make sure that all relevant users have phone numbers that are listed for them in the directory.

Procedure

Step 1 From Cisco Unified CallManager Administration, choose **User Management > End User**.

The Find and List Users window displays.

Step 2 In the User Search field, enter the appropriate search criteria and click **Find**.

Step 3 From the resulting list of matching names, click the name of the user to which you want to add a phone number.

Step 4 In the Telephone Number field, enter the user telephone number.

Step 5 Click **Save**.

Voice-Messaging Issues

This section addresses the problem of the incorrect voice-messaging greeting being played.

Symptom

When a call is not answered at the attendant and forwarded to voice-messaging, the voice-messaging system plays the attendant greeting instead of the pilot point greeting.

Possible Cause

The Reset Original Called service parameter specifies True.

Recommended Action

Use the following procedure to set the service parameter to the proper value.

Procedure

Step 1 Choose **System > Service Parameters**.

Step 2 From the Server drop-down list box, choose the Attendant Console server.

Step 3 From the Service drop-down list box, choose the Cisco CallManager Attendant Console service.

Step 4 From the Reset Original Called drop-down list box, choose False.

Problems Using Cisco Unified CallManager Attendant Console Interface

This section addresses the following Cisco Unified CallManager Attendant Console interface issues:

- Unable to Communicate with Cisco Unified CallManager Attendant Console Server, page 8-18
- Text Displays Incorrect Language, page 8-19
- Cannot Search for Unicode Languages, page 8-19
- Speed-Dial and Directory Windows Display Incorrect Line State, page 8-20
- Directory Numbers Appear in an Unknown Line State, page 8-20

Unable to Communicate with Cisco Unified CallManager Attendant Console Server

Symptom

When the attendant attempted to log in to the attendant console, a dialog box stated that the attendant console was unable to communicate to the server.

Possible Cause

The attendant console client and the attendant console server do not reside in the same domain.

Recommended Action

Enter the mapping of the IP address and the fully qualified domain name of the server in the hosts file of attendant console client.

Procedure

Step 1 From the Cisco Unified CallManager Attendant Console PC, open the hosts file located at c:\program files\winnt\system32\drivers\etc\hosts.

Step 2 Make an entry for the IP address and fully qualified hostname of the server.

To make an entry for server with the IP address of 10.104.1.4 and a domain name of tbd2-pub-7835.cluster1.com, make the following entry:

```
10.104.1.4 tbd2-pub-7835.cluster1.com
```

Text Displays Incorrect Language

Symptom

Some text displays in English, while other text displays in the language that the attendant chose in the Cisco Unified CallManager Attendant Console dialog box.

Probable Cause

The latest locale installer that is available for the chosen language is not installed.

Corrective Action

You must install the latest locale installer that is available for your chosen language. Refer the *Cisco Unified Communications Operating System Administration* documentation that is available on the web.

Cannot Search for Unicode Languages

Symptom

You cannot search for unicode languages such as Japanese in the directory of Cisco Unified IP Phones and applications such as Cisco Unified CallManager Attendant Console.

Possible Cause

Cisco Unified IP Phones and certain applications do not support unicode languages.

Recommended Action

To enable directory searching capabilities, enter the pronunciation of the name in ASCII text and an ellipsis (...) in front of the unicode name in the first and last name fields of the End User Configuration window in Cisco Unified CallManager Administration. The phone or application can search on the ASCII text version of the name. If you use the advanced search capability in Cisco Unified CallManager Attendant Console, you can search for either the ASCII name or the Unicode name.

Speed-Dial and Directory Windows Display Incorrect Line State

Symptom

The Speed Dial window and the Directory window do not display the correct line state.

Possible Cause

Line state updates from the server to the client get sent by using UDP packets. If a NAT device or a firewall separates the client and server, the client most likely does not receive line state updates from the server.

Recommended Action

Ensure that both client and server are on the same side of the NAT device or the firewall.

Directory Numbers Appear in an Unknown Line State

Symptom

Line states of some directory numbers appear in an unknown state.

Possible Cause

The Cisco CallManager Attendant Console Server service does not start on all Cisco Unified CallManager servers from which the phones receive call-processing services.

Recommended Action

Activate and start the Cisco CallManager Attendant Console Server service on all Cisco Unified CallManager servers from which the phones receive call-processing services. For information on activating services, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Cisco Unified CallManager Serviceability Does Not Generate JTAPI Logs

This section addresses the issue of JTAPI logs not generating.

Symptom

You changed the trace level from Error to Detailed, but the JTAPI logs still do not get generated.

Possible Cause

JTAPI trace levels are set at the initialization time of JTAPI and are not changed later.

Recommended Action

Restart the Cisco CallManager Attendant Console Server service. For information on restarting services, refer to the *Cisco Unified CallManager Serviceability Administration Guide*

Collecting Server Logs

This section addresses how to collect server logs:

Symptom

Need a solution to collect all server-side logs.

Possible Cause

To debug server issues, collect the following traces:

- CCM
- CTI
- SDL CCM
- SDL CTI
- Cisco CallManager Attendant Console Server
- JTAPI

Recommended Action

Use Cisco Unified Real-Time Monitoring Tool (RTMT) or the CLI to collect the appropriate log files. For information on RTMT, refer the *Cisco Unified CallManager Serviceability Administration Guide*. For information on CLI commands, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Performance Monitor Counters for Cisco Unified CallManager Attendant Console

Performance monitor counters for Cisco Unified CallManager Attendant Console in real-time monitoring tool (RTMT) allow you to monitor the time that Cisco CallManager Attendant Console Server service has been running, the amount of time since the Cisco CallManager Attendant Console Server service was started, the number of calls that have occurred, the number of calls that have been redirected, the number of attendants that are registered, the number of pilot points, and the number of registered clients.

The CcmLineLinkState performance monitor for the attendant console provides a quick way to check whether the attendant console is functioning correctly:

- If the CcmLineLinkState counter is 11, this state indicates that Cisco CallManager Attendant Console Server service is functioning normally.
- The left-most digit of CcmLineLinkState indicates whether Cisco CallManager Attendant Console Server service is connected to and registered with the Cisco Unified CallManager CTI. If this digit is 0, a problem may exist with the CTI or the directory.
- The right-most digit of CcmLineLinkState indicates whether Cisco CallManager Attendant Console Server service can perceive line state information through Cisco Unified CallManager. If this digit is 0, a problem probably exists with Cisco Unified CallManager.

Note When an attendant console user cannot log in to the attendant console and no line state information is available, view the CcmLineLinkState performance monitor to verify that all components of attendant console are functioning properly.

For more information about performance monitor counters and alarms, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

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.

Probable 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

Step 1 From Cisco Unified CallManager Administration, go to **Device > Phone** and click **Find the phone** to find the phone configuration of the phone that is having the problem.

Step 2 Set the Built In Bridge parameter to On.

Step 3 Click Update.

Step 4 Reset the phone.

Troubleshooting Immediate Divert

This section covers solutions for the following most common issues that relate to the Immediate Divert feature.

- Key is not active, page 8-24
- Temporary Failure, page 8-24
- Busy, page 8-24

Key is not active

Symptom

This message displays on the phone when the user presses iDivert.

Probable 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.

Probable 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.

Probable Cause

Message means that the voice-messaging system is busy.

Corrective Action

Configure more voice-messaging ports or try again.

Troubleshooting Cisco WebDialer

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

Authentication Error

Symptom

Cisco WebDialer 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 using your Cisco Unified CallManager userID and password.

Service Temporarily Unavailable

Symptom

Cisco WebDialer displays the following message:

Service temporarily unavailable, please try again later.

Probable 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 WebDialer displays the following message:

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

Probable Cause

The Cisco CallManager directory service may be down.

Corrective Action

After a short time, retry your connection.

Cisco CTIManager Down

Symptom

Cisco WebDialer displays the following message:

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

Probable Cause

Cisco CTIManager service that is configured for Cisco WebDialer went down.

Corrective Action

After a short time, retry your connection.

Session Expired, Please Login Again

Symptom

Cisco WebDialer displays the following message:

Session expired, please login again.

Probable Cause

A Cisco WebDialer session expires

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

Corrective Action

Log in by using your Cisco Unified CallManager userID and password.

User Not Logged in on Any Device

Symptom

Cisco WebDialer displays the following message:

User not logged in on any device.

Probable Cause

The user chooses to use Cisco Extension Mobility from the Cisco WebDialer preference page but is not logged into any IP phone.

Corrective Action

- Log in to a phone before using Cisco WebDialer.
- Choose a device from the Cisco WebDialer 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 WebDialer displays the following message:

User not logged in on any device.

Probable Cause

- The user chose a Cisco Unified IP Phone that is not registered with Cisco Unified CallManager. 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 Cisco Unified CallManager.

Destination Not Reachable

Symptom

Cisco WebDialer displays the following message on the End Call window:

Destination not reachable.

Probable 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 Cisco Call Back

This section provides symptoms, possible causes, recommended actions, and error messages when Cisco Call Back does not work as expected. This section provides information on the following topics:

- Problems Using Cisco Call Back, page 8-28
- Error Messages for Cisco Call Back, page 8-29
- Locating the Cisco Call Back Log Files, page 8-30

Problems Using Cisco 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.

Probable 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 Cisco Call Back is activated.

Probable 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 Cisco 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.

Probable 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, Cisco 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.

Probable 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.

Probable 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 Cisco 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 Cisco Unified CallManager 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 Cisco Call Back Log Files

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

APPENDIX A

Opening a Case With TAC

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

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:

- Information You Will Need, page A-2
- Required Preliminary Information, page A-2
- Online Cases, page A-3
- Cisco Live!, page A-4
- Remote Access, page A-4
- Cisco Secure Telnet, page A-4

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 upon the engineer's request after opening a case inevitably results in resolution delay.

- Required Preliminary Information
  - Network Layout
  - Problem Description
  - General Information
- Online Cases
- Cisco Live!
- Remote Access
- Cisco Secure Telnet

Required Preliminary Information

For all issues, always provide the following information to TAC. Collect and save this information for use upon opening a TAC case and update it regularly with any changes.

- Network Layout
- Problem Description
- General Information

Network Layout

Provide a detailed description of the physical and logical setup, as well as all the following network elements involved in the voice network (if applicable):

- Cisco Unified CallManager(s)
  - Version (from Cisco Unified CallManager Administration choose **Details**)
  - Number of Cisco Unified CallManagers
  - Setup (stand-alone, cluster)
- Unity
  - Version (from the Cisco Unified CallManager Administration)
  - Integration type
- Applications
  - List of installed applications
  - Version numbers of each application
- IP/voice gateways
  - OS version

- Show tech (IOS gateway)
- Cisco Unified CallManager load (Skinny gateway)

- Switch
  - OS version
  - VLAN configuration
- Dial plan—Numbering scheme, call routing

Ideally, submit a Visio or other detailed diagram, such as JPG. Using the whiteboard, you may also provide the diagram through a Cisco Live! session.

Problem Description

Provide step-by-step detail of actions that the user performed when the issue occurs. Ensure the detailed information includes

- Expected behavior
- Detailed observed behavior

General Information

Make sure that the following information is readily available:

- Is this a new installation?
- If this is a previous version of a Cisco Unified CallManager installation, has this issue occurred since the beginning? (If not, what changes were recently made to the system?)
- Is the issue reproducible?
  - If reproducible, is it under normal or special circumstances?
  - If not reproducible, is there anything special about when it does occur?
  - What is the frequency of occurrence?
- What are the affected devices?
  - If specific devices are affected (not random), what do they have in common?
  - Include DNs or IP addresses (if gateways) for all devices that are involved in the problem.
- What devices are on the Call-Path (if applicable)?

Online Cases

Opening an 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 CCO case. That description of the problem returns URL links that may provide you with an immediate solution.

If you do not find a solution to your problem, continue the process of sending your case to a TAC engineer.

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 Cisco Unified CallManager servers on your site.

Cisco Secure Telnet works by enabling a Telnet client inside the Cisco Systems firewall to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and maintenance of your Cisco Unified CallManager servers without requiring firewall modifications.

Note Cisco accesses your network only with your permission. You must provide a network administrator at your site to help initiate the process.

Firewall Protection

Virtually all internal networks use firewall applications to restrict outside access to internal host systems. These applications protect your network by restricting IP connections between the network and the public Internet.

Firewalls work by automatically blocking TCP/IP connections that are initiated from the outside, unless the software is reconfigured to allow such access.

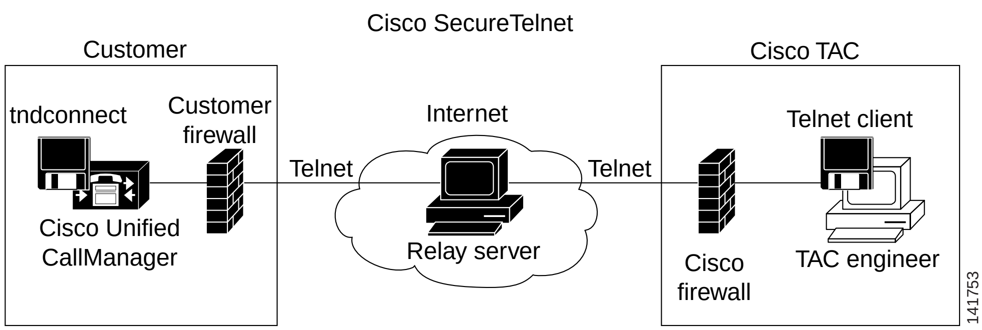
Corporate networks normally permit communication with the public Internet but only if connections directed to outside hosts originate from inside the firewall.

Cisco Secure Telnet Design

Cisco Secure Telnet takes advantage of the fact that Telnet connections can easily be initiated from behind a firewall. Using an external proxy machine, the system relays TCP/IP communications from behind your firewall to a host behind another firewall at the Cisco Technical Assistance Center (TAC).

Using this relay server maintains the integrity of both firewalls while secure communication between the shielded remote systems get supported.

Figure A-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 Cisco Unified CallManager server to your CSE.

Note The password comprises a text string upon which your administrator and the CSE mutually agree.

Your administrator starts the process by initiating the Telnet tunnel, which establishes a TCP connection from inside your firewall out to the relay server on the public Internet. The Telnet tunnel then establishes another connection to your local Telnet server, creating a two-way link between the entities.

Note The Telnet client at the Cisco TAC runs in compliance with systems that run on Windows NT and Windows 2000 or with UNIX operating systems.

After the Cisco CallManager at your site accepts the password, the Telnet client that is running at the Cisco TAC connects to the Telnet daemon that is running behind your firewall. The resulting transparent connection allows the same access as if the machine were being used locally.

After the Telnet connection is stable, the CSE can implement all remote serviceability functionality to perform maintenance, diagnostic, and troubleshooting tasks on your Cisco Unified CallManager server.

You can view the commands that the CSE sends and the responses that your Cisco Unified CallManager server issues, but the commands and responses may not always be completely formatted.

Case Study: Troubleshooting Cisco Unified IP Phone Calls

This appendix contains two case studies:

- Troubleshooting Intracluster Cisco Unified IP Phone Calls
- Troubleshooting Intercluster Cisco Unified IP Phone Calls

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 Cisco Unified CallManager and Cisco Unified IP Phone initialization, registration, and keepalive processes. A detailed explanation of an intracluster call flow follows the discussion. The explanation of the processes uses the trace utilities and tools that are discussed in Chapter 2, "Troubleshooting Tools."

This section contains the following topics:

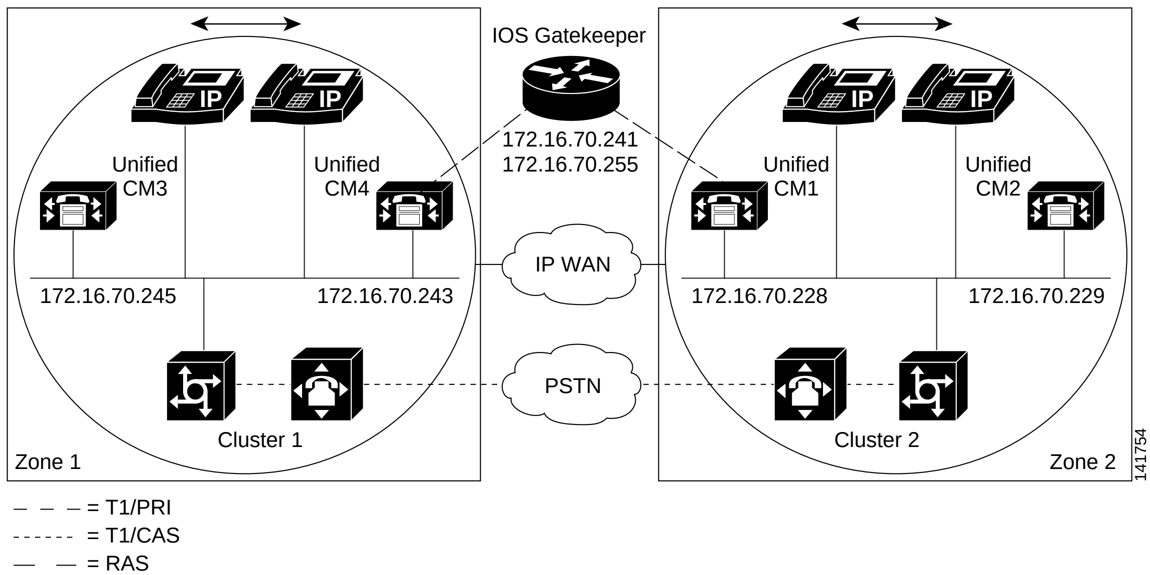
- Sample Topology
- Cisco Unified IP Phone Initialization Process
- Cisco Unified CallManager Initialization Process
- Self-Starting Processes
- Cisco Unified CallManager Registration Process
- Cisco Unified CallManager KeepAlive Process
- Cisco Unified CallManager Intracluster Call Flow Traces

Sample Topology

You have two clusters that are named Cluster 1 and Cluster 2; the two Cisco Unified CallManagers in Cluster 1 are called Unified CM3 and Unified CM4, while the two Cisco Unified CallManagers 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 Figure B-1. 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 B-1 Sample Topology of Intracluster Cisco IP Phone-to-Cisco 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

Step 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).

Step 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.

Step 3 If the DHCP reply does not include a TFTP server name, the Cisco IP Phone uses the default server name.

Step 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 Cisco Unified CallManager, 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).

Step 5 All .cnf files include the IP address(es) for the primary and secondary Cisco Unified CallManager(s). The Cisco Unified IP Phone uses this IP address to contact the primary Cisco Unified CallManager and to register.

Step 6 After the Cisco Unified IP Phone connects and registers with Cisco Unified CallManager, the Cisco Unified CallManager 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 CallManager Initialization Process

This section explains the initialization process of Cisco Unified CallManager with the help of traces that are captured from Unified CM1 (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 Cisco Unified CallManager is initialized. Understanding how to read traces will help you to properly troubleshoot the various Cisco Unified CallManager processes and the effect of those processes on services such as conferencing and call forwarding.

The following messages from the Cisco Unified CallManager SDI trace utility show the initialization process on one of the Cisco Unified CallManagers, in this case, Unified CM1.

- The first message indicates that Cisco Unified CallManager started its initialization process.
- The second message indicates that Cisco Unified CallManager read the default database values (for this case, it is the primary or publisher database).
- The third message indicates Cisco Unified CallManager received the various messages on TCP port 8002.
- The fourth message shows that, after receiving to these messages, Cisco Unified CallManager added a second Cisco Unified CallManager to its list: Unified CM2 (172.16.70.229).
- The fifth message indicates that Cisco Unified CallManager has started and is running Cisco Unified CallManager version 3.1(1).

```
16:02:47.765 CCM|CMProcMon - CallManagerState 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 Cisco Unified CallManager is up and running, it starts several other processes within itself. Some of these processes follow, including MulticastPoint Manager, UnicastBridge Manager, digit analysis, and route list. You will find 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 Cisco Unified CallManager.

For example, assume that the route lists are not functioning and are unusable. To troubleshoot this problem, you would monitor these traces to determine whether the Cisco Unified CallManager 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 - Started
```

```
16:02:51.031 CCM|UnicastBridgeManager - Started
16:02:51.031 CCM|MediaTerminationPointManager - Started
16:02:51.125 CCM|MediaCoordinator(1) - started
16:02:51.125 CCM|NodeId:    1, EventId: 1543 EventClass:  2 EventInfo: Database manager
started
16:02:51.234 CCM|NodeId:    1, EventId: 1542 EventClass:  2 EventInfo: Link manager
started
16:02:51.390 CCM|NodeId:    1, EventId: 1541 EventClass:  2 EventInfo: Digit analysis
started
16:02:51.406 CCM|RoutePlanManager - Started, loading RouteLists
16:02:51.562 CCM|RoutePlanManager - finished loading RouteLists
16:02:51.671 CCM|RoutePlanManager - finished loading RouteGroups
16:02:51.671 CCM|RoutePlanManager - Displaying Resulting RoutePlan
16:02:51.671 CCM|RoutePlanServer - RouteList Info, by RouteList and RouteGroup Selection
Order
16:02:51.671 CCM|RouteList - RouteListName=''ipwan''
16:02:51.671 CCM|RouteList - RouteGroupName=''ipwan''
16:02:51.671 CCM|RoutePlanServer - RouteGroup Info, by RouteGroup and Device Selection
Order
16:02:51.671 CCM|RouteGroup - RouteGroupName=''ipwan''
```

The following trace shows the RouteGroup 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 Cisco Unified CallManager is adding "Dns" (Directory Numbers). By reviewing these messages, you can determine whether the Cisco Unified CallManager read the directory number from the database.

```
16:02:51.671 CCM|NodeId:    1, EventId: 1540 EventClass:  2 EventInfo: Call control
started
16:02:51.843 CCM|ProcessDb -        Dn = 2XXX,      Line = 0,    Display = ,
RouteThisPattern, NetworkLocation = OffNet, DigitDiscardingInstruction = 1, WhereClause =
16:02:51.859 CCM|Digit analysis: Add local pattern 2XXX , PID: 1,80,1
16:02:51.859 CCM|ForwardManager - Started
16:02:51.984 CCM|CallParkManager - Started
16:02:52.046 CCM|ConferenceManager - Started
```

In the following traces, the Device Manager in Cisco Unified CallManager statically initializes two devices. The device with IP address 172.17.70.226 represents a gatekeeper, and the device with IP address 172.17.70.245 gets another Cisco Unified CallManager in a different cluster. That Cisco Unified CallManager gets registered as an H.323 Gateway with this Cisco Unified CallManager.

```
16:02:52.250 CCM|DeviceManager: Statically Initializing Device;  DeviceName=172.16.70.226
16:02:52.250 CCM|DeviceManager: Statically Initializing Device;  DeviceName=172.16.70.245
```

Cisco Unified CallManager Registration Process

Another important part of the SDI trace involves the registration process. When a device is powered up, it gets information via DHCP, connects to the TFTP server for its .cnf file, and then connects to the Cisco Unified CallManager 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, Cisco Unified CallManager 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 Cisco Unified CallManager, they get treated internally as different external services and therefore get assigned a TCPHandle, socket number, and port number as well as a device name.

```
16:02:52.750 CCM|StationInit - New connection accepted. DeviceName=, TCPHandle=0x4fbaa00,
Socket=0x594, IPAddr=172.16.70.228, Port=3279, StationD=[0,0,0]
16:02:52.750 CCM|StationInit - New connection accepted. DeviceName=, TCPHandle=0x4fe05e8,
Socket=0x59c, IPAddr=172.16.70.228, Port=3280, StationD=[0,0,0]
16:02:52.781 CCM|StationInit - Processing StationReg. regCount: 1 DeviceName=MTP_nsa-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 CallManager KeepAlive Process

The station, device, or service and the Cisco Unified CallManager use the following messages to maintain a knowledge of the communications channel between them. The messages begin the keepalive sequence that ensures that the communications link between the Cisco Unified CallManager and the station remains active. The following messages can originate from either the Cisco Unified CallManager or the station.

```
16:03:02.328 CCM|StationInit - InboundStim - KeepAliveMessage - Forward KeepAlive to
StationD. DeviceName=MTP_nsa-cm2, TCPHandle=0x4fa7dc0, Socket=0x568, IPAddr=172.16.70.229,
Port=1556, StationD=[1,45,1]
16:03:02.328 CCM|StationInit - InboundStim - KeepAliveMessage - Forward KeepAlive to
StationD. DeviceName=CFB_nsa-cm2, TCPHandle=0x4bf8a70, Socket=0x57c, IPAddr=172.16.70.229,
Port=1557, StationD=[1,96,1]
16:03:06.640 CCM|StationInit - InboundStim - KeepAliveMessage - Forward KeepAlive to
StationD. DeviceName=SEP0010EB001720, TCPHandle=0x4fbb150, Socket=0x600,
IPAddr=172.16.70.230, Port=49211, StationD=[1,85,2]
16:03:06.703 CCM|StationInit - InboundStim - KeepAliveMessage - Forward KeepAlive to
StationD. DeviceName=SEP003094C26105, TCPHandle=0x4fbbc30, Socket=0x5a4,
IPAddr=172.16.70.231, Port=52095, StationD=[1,85,1]
```

The messages in the following trace depict the keepalive sequence that indicates that the communications link between the Cisco Unified CallManager and the station is active. Again, these messages can originate from either the Cisco Unified CallManager or the station.

```
16:03:02.328 CCM|MediaTerminationPointControl - stationOutputKeepAliveAck
tcpHandle=4fa7dc0
16:03:02.328 CCM|UnicastBridgeControl - stationOutputKeepAliveAck tcpHandle=4bf8a70
16:03:06.703 CCM|StationInit - InboundStim - IpPortMessageID: 32715(0x7fcb)
tcpHandle=0x4fbbc30
16:03:06.703 CCM|StationD - stationOutputKeepAliveAck tcpHandle=0x4fbbc30
```

Cisco Unified CallManager Intracluster Call Flow Traces

The following SDI traces explore the intracluster call flow in detail. You can identify Cisco Unified IP Phones 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. Thefollowing information displays in the form of Skinny Station messages between the Cisco Unified IP Phones and the Cisco Unified CallManager.

```
16:05:41.625 CCM|StationInit - InboundStim - OffHookMessageID tcpHandle=0x4fbbc30
16:05:41.625 CCM|StationD - stationOutputDisplayText tcpHandle=0x4fbbc30, Display= 1001
```

The next trace shows Skinny Station messages that go from Cisco Unified CallManager 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
```

Cisco Unified CallManager uses the stationOutputCallState message to notify the station of certain call-related information.

```
16:05:41.625 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
```

Cisco Unified CallManager uses 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
```

Cisco Unified CallManager uses the stationOutputSelectSoftKey message to cause the Skinny Station to choose a specific set of soft keys.

```
16:05:41.625 CCM|StationD - stationOutputSelectSoftKeys tcpHandle=0x4fbbc30
```

Cisco Unified CallManager 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, Cisco Unified CallManager sends StationD messages, and Cisco Unified CallManager performs digit analysis.

```
16:05:41.625 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="")
16:05:41.625 CCM|Digit analysis: potentialMatches=PotentialMatchesExist
```

The following debug message shows that the Cisco Unified CallManager 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 Cisco Unified CallManager 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=0x4fbbc30
16:05:42.890 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
16:05:42.890 CCM|StationD - stationOutputSelectSoftKeys tcpHandle=0x4fbbc30
16:05:42.890 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="1")
16:05:42.890 CCM|Digit analysis: potentialMatches=PotentialMatchesExist
16:05:43.203 CCM|StationInit - InboundStim - KeypadButtonMessageID kpButton: 0
tcpHandle=0x4fbbc30
16:05:43.203 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="10")
16:05:43.203 CCM|Digit analysis: potentialMatches=PotentialMatchesExist
```

```
16:05:43.406 CCM|StationInit - InboundStim - KeypadButtonMessageID kpButton: 0
tcpHandle=0x4fbbc30
16:05:43.406 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="100")
16:05:43.406 CCM|Digit analysis: potentialMatches=PotentialMatchesExist
16:05:43.562 CCM|StationInit - InboundStim - KeypadButtonMessageID kpButton: 0
tcpHandle=0x4fbbc30
16:05:43.562 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="1000")
```

After the Cisco Unified CallManager receives enough digits to match, it provides the digit analysis results in a table format. Cisco Unified CallManager 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 results
16:05:43.562 CCM||PretransformCallingPartyNumber=1001
|CallingPartyNumber=1001
|DialingPattern=1000
|DialingRoutePatternRegularExpression=(1000)
|PotentialMatches=PotentialMatchesExist
|DialingSdlProcessId=(1,38,2)
|PretransformDigitString=1000
|PretransformPositionalMatchList=1000
|CollectedDigits=1000
|PositionalMatchList=1000
|RouteBlockFlag=RouteThisPattern
```

The next trace shows that Cisco Unified CallManager is sending out this information to a called party phone (the tcpHandle number identifies the phone).

```
16:05:43.578 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=1000, CalledParty=1000, tcpHandle=0x4fbb150
```

The next trace indicates that Cisco Unified CallManager 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, Cisco Unified CallManager 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=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputDisplayNotify tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputDisplayPromptStatus tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputSelectSoftKeys tcpHandle=0x4fbb150
```

Notice that Cisco Unified CallManager 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=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=1000, CalledParty=1000, tcpHandle=0x4fbbc30
```

In the next trace, Cisco Unified CallManager 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=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputSelectSoftKeys tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputDisplayPromptStatus tcpHandle=0x4fbbc30
```

At this point, the called party Cisco Unified IP Phone goes off hook; therefore, Cisco Unified CallManager stops generating the ringer tone to calling party.

```
16:05:45.140 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
```

In the following messages, Cisco Unified CallManager causes the Skinny Station to begin receiving a Unicast RTP stream. To do so, Cisco Unified CallManager provides the IP address of the called party as well as codec information and packet size in msec (milliseconds). PacketSize designates an integer that contains the sampling time, in milliseconds, that is used to create the RTP packets.

Note 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, Cisco Unified CallManager provides information to the called party (1000).

```
16:05:45.140 CCM|StationD - stationOutputOpenReceiveChannel tcpHandle=0x4fbb150 myIP:
e64610ac (172.16.70.230)
16:05:45.140 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
```

Cisco Unified CallManager received the acknowledgment message from called party for establishing the open channel for RTP stream, as well as the IP address of the called party. This message informs the Cisco Unified CallManager of two pieces of information about the Skinny Station. First, it contains the status of the open action. Second, it contains the receive port address and number for transmission to the remote end. The IP address of the transmitter (calling part) of the RTP stream 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
```

Cisco Unified CallManager 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 Cisco IP Phone finally goes on hook, which terminates all the control messages between the Skinny Station and Cisco Unified CallManager 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.

This section contains the following topics:

- Sample Topology
- Intercluster H.323 Communication
- Call Flow Traces
- Failed Call Flow

Sample Topology

The following sample topology gets used in this case study. Two clusters, each having two Cisco Unified CallManagers, and also Cisco IOS Gateways and a Cisco IOS Gatekeeper are in place.

Intercluster H.323 Communication

The Cisco IP Phone in Cluster 1 makes a call to the Cisco Unified IP Phone in Cluster 2. Intercluster Cisco Unified CallManager 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 Cisco Unified CallManager via Skinny Station protocol, and the Cisco Unified CallManager can connect with the Cisco IOS Gatekeeper by using the H.323 Registration, Admission, and Status (RAS) protocol. The admission request message (ARQ) gets sent to the Cisco IOS Gatekeeper, which sends the admission confirmed message (ACF) after making sure 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=0x1c64310
16:06:13.953 CCM|Out Message -- H225ConnectMsg -- Protocol= H225Protocol
16:06:13.953 CCM|Ie - H225UserUserIe IEData= 7E 00 37 05 02 C0 06
16:06:13.953 CCM|StationD - stationOutputCallInfo CallingPartyName=,  CallingParty=2002,
CalledPartyName=1001, CalledParty=1001, tcpHandle=0x1c64310
16:06:14.015 CCM|H245Interface(2) OLC indication chan number = 2
16:06:14.015 CCM|StationD - stationOutputOpenReceiveChannel tcpHandle=0x1c64310 myIP:
e74610ac (172.16.70.231)
16:06:14.015 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
16:06:14.062 CCM|StationInit - InboundStim - StationOpenReceiveChannelAckID
tcpHandle=0x1c64310, Status=0, IpAddr=0xe74610ac, Port=20444, PartyID=2
16:06:14.062 CCM|H245Interface(2) paths established ip = e74610ac, port = 20444
16:06:14.187 CCM|H245Interface(2) OLC outgoing confirm ip = fc4610ac, port = 29626
```

The following traces show the calling and called party number, which associates with an IP address and a 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 IP Phone (2002). The disconnect, then on-hook messages, follow these traces.

```
RemoteRtpPortNumber: 29626 msecPacketSize: 20 compressionType:(4)Media_Payload_G711Ulaw64k
16:06:16.515 CCM| Device SEP003094C26105 , UnRegisters with SDL Link to monitor NodeID= 1
16:06:16.515 CCM|StationD - stationOutputCloseReceiveChannel tcpHandle=0x1c64310 myIP:
e74610ac (172.16.70.231)
16:06:16.515 CCM|StationD - stationOutputStopMediaTransmission tcpHandle=0x1c64310 myIP:
e74610ac (172.16.70.231)
16:06:16.531 CCM|In  Message -- H225ReleaseCompleteMsg -- Protocol= H225Protocol
16:06:16.531 CCM|Ie - Q931CauseIe -- IEData= 08 02 80 90
16:06:16.531 CCM|Ie - H225UserUserIe -- IEData= 7E 00 1D 05 05 80 06
16:06:16.531 CCM|Locations:Orig=1 BW=64Dest=0 BW=-1 (-1 implies infinite bw available)
16:06:16.531 CCM|MediaManager - wait_AuDisconnectRequest - StopSession sending disconnect
to (64,2) and remove connection from list
16:06:16.531 CCM|MediaManager - wait_AuDisconnectReply - received all disconnect replies,
forwarding a reply for party1(16777219) and party2(16777220)
16:06:16.531 CCM|MediaCoordinator - wait_AuDisconnectReply - removing MediaManager(2) from
connection list
16:06:16.734 CCM|StationInit - InboundStim - OnHookMessageID tcpHandle=0x1c64310
```

Failed Call Flow

The following section describes an unsuccessful intercluster call flow, as seen in the SDI trace. In the following traces, the Cisco 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=0x4fbbc30
16:05:33.468 CCM|StationD - stationOutputDisplayText tcpHandle=0x4fbbc30, Display= 1001
16:05:33.484 CCM|StationD - stationOutputSetLamp stim: 9=Line instance=1 lampMode=LampOn
tcpHandle=0x4fbbc30
```

In the following traces, the user dials the called number (2000) of the Cisco 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 Cisco Unified CallManager cannot match this directory number. Finally, a reorder tone gets sent to the calling party (1001), which is followed by an on-hook message.

```
16:05:36.812 CCM|Digit analysis: analysis results
16:05:36.812 CCM||PretransformCallingPartyNumber=1001
|CallingPartyNumber=1001
|DialingPattern=2XXX
|DialingRoutePatternRegularExpression=(2XXX)
|PotentialMatches=NoPotentialMatchesExist
|CollectedDigits=2000
16:05:36.828 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=2000, tcpHandle=0x4fbbc30
16:05:36.828 CCM|StationD - stationOutputStartTone: 37=ReorderTone tcpHandle=0x4fbbc30
16:05:37.953 CCM|StationInit - InboundStim - OnHookMessageID tcpHandle=0x4fbbc30
```

Case Study: Troubleshooting Cisco Unified IP Phone-to-Cisco IOS Gateway Calls

The case study described in Appendix B, "Case Study: Troubleshooting Cisco Unified IP Phone Calls," describes the call flow for an intracluster call. The case study in this appendix examines a Cisco Unified IP Phone that is calling through a Cisco IOS Gateway to a phone that connectes 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.

This section contains the following topics:

- Call Flow Traces
- Debug Messages and Show Commands on the Cisco IOS Gatekeeper
- Debug Messages and Show Commands on the Cisco IOS Gateway
- Cisco IOS Gateway with T1/PRI Interface
- Cisco IOS Gateway with T1/CAS Interface

Call Flow Traces

This section discusses call flow through examples from the Cisco CallManager trace file CCM000000000. The traces in this case study focus only on the call flow itself because Appendix B, "Case Study: Troubleshooting Cisco Unified IP Phone Calls," (for example, initialization, registration, and keepalive mechanism) already explained the more detailed trace information.

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. 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 Cisco Unified CallManager currently active analyzes the digits to discover where the call needs to get routed. Appendix B, "Case Study: Troubleshooting Cisco Unified IP Phone Calls," provides a more detailed explanation of the digit analysis

```
15:20:18.390 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="")
15:20:19.703 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="3")
15:20:20.078 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="33")
15:20:20.718 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="333")
15:20:21.421 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="3333")
15:20:21.421 CCM|Digit analysis: analysis results
```

In the following traces, the digit analysis 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= H225Protocol
15:20:21.421 CCM|MMan_Id= 1. (iep=  0 dsl=  0 sapi=  0 ces=  0 IpAddr=e24610ac
IpPort=47110)
```

The following trace shows the calling and called party information as well as the H.225 alerting message. The trace also shows is the mapping of a Cisco Unified IP Phone hexidecimal value to the IP address. The IP address of the Cisco Unified IP Phone (1001) specifies 172.16.70.231.

```
15:20:21.437 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=3333, tcpHandle=0x5138d98
15:20:21.453 CCM|In  Message -- H225AlertMsg -- Protocol= H225Protocol
15:20:21.953 CCM|StationD - stationOutputOpenReceiveChannel tcpHandle=0x5138d98 myIP:
e74610ac (172.16.70.231)
```

The following trace shows the compression type that is used for this call (G.711 mu-law).

```
15:20:21.953 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
```

After the H.225 alert message 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= H225Protocol
15:20:22.968 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=3333, tcpHandle=0x5138d98
15:20:22.062 CCM|MediaCoordinator - wait_AuConnectInfoInd
15:20:22.062 CCM|StationD - stationOutputStartMediaTransmission tcpHandle=0x5138d98 myIP:
e74610ac (172.16.70.231)
15:20:22.062 CCM|StationD - RemoteIpAddr: e24610ac (172.16.70.226) RemoteRtpPortNumber:
16758 msecPacketSize: 20 compressionType:(4)Media_Payload_G711Ulaw64k
15:20:22.062 CCM|Locations:Orig=0 BW=-1Dest=1 BW=6(-1 implies infinite bw available)
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=0x5138d98
```

```
15:20:27.296 CCM|ConnectionManager -wait_AuDisconnectRequest (16777247,16777248): STOP
SESSION
15:20:27.296 CCM|MediaManager - wait_AuDisconnectRequest - StopSession sending disconnect
to (64,5) and remove connection from list
15:20:27.296 CCM| Device SEP003094C26105 , UnRegisters with SDL Link to monitor NodeID= 1
15:20:27.296 CCM|StationD - stationOutputCloseReceiveChannel tcpHandle=0x5138d98 myIP:
e74610ac (172.16.70.231)
15:20:27.296 CCM|StationD - stationOutputStopMediaTransmission tcpHandle=0x5138d98 myIP:
e74610ac (172.16.70.231)
15:20:28.328 CCM|In  Message -- H225ReleaseCompleteMsg -- Protocol= H225Protocol
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>
```

Debug Messages and Show Commands on the Cisco IOS Gatekeeper

The "Call Flow Traces" section on page C-1 covers the Cisco Unified CallManager SDI trace in detail. In the topology for this case study, the debug ras command turned on in the Cisco IOS Gatekeeper.

The following debug messages show that the Cisco IOS Gatekeeper is receiving the admission request (ARQ) for the Cisco Unified CallManager (172.16.70.228), followed by other successful Remote Access Server (RAS) messages. Finally, the Cisco IOS Gatekeeper sends an admission confirmed (ACF) message to the Cisco Unified CallManager.

```
*Mar 12 04:03:57.181: RASLibRASRecvData ARQ (seq# 3365) rcvd from [172.16.70.228883] on
sock [0x60AF038C]
*Mar 12 04:03:57.181: RASLibRAS_WK_TInit ipsock [0x60A7A68C] setup successful
*Mar 12 04:03:57.181: RASlibras_sendto msg length 16 from 172.16.70.2251719 to
172.16.70.228883
*Mar 12 04:03:57.181: RASLibRASSendACF ACF (seq# 3365) sent to 172.16.70.228
```

The following debug messages show that the call is in progress.

```
*Mar 12 04:03:57.181: RASLibRASRecvData successfully rcvd message of length 55 from
172.16.70.228883
```

The following debug messages show that the Cisco IOS Gatekeeper received a disengage request (DRQ) from the Cisco Unified CallManager (172.16.70.228), and the Cisco IOS Gatekeeper sent a disengage confirmed (DCF) to the Cisco Unified CallManager.

```
*Mar 12 04:03:57.181: RASLibRASRecvData DRQ (seq# 3366) rcvd from [172.16.70.228883] on
sock [0x60AF038C]
```

```
*Mar 12 04:03:57.181: RASlibras_sendto msg length 3 from 172.16.70.2251719 to
172.16.70.228883
*Mar 12 04:03:57.181: RASLibRASSendDCF DCF (seq# 3366) sent to 172.16.70.228
*Mar 12 04:03:57.181: RASLibRASRecvData successfully rcvd message of length 124 from
172.16.70.228883
```

The command show gatekeeper endpoints on the Cisco IOS Gatekeeper shows that all four Cisco Unified CallManagers are registered with the Cisco IOS Gatekeeper. In the topology for this case study, four Cisco Unified CallManagers exist, two in each cluster. This Cisco IOS Gatekeeper includes two zones, and each zone includes two Cisco Unified CallManagers.

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
```

Debug Messages and Show Commands on the Cisco IOS Gateway

The “Debug Messages and Show Commands on the Cisco IOS Gatekeeper” section on page C-4 discusses the Cisco IOS Gatekeeper show commands and debug outputs were discussed in detail. This section focuses on the debug output and show commands on the Cisco IOS Gateway. In the topology for this case study, calls go through the Cisco IOS Gateways. The Cisco IOS Gateway interfaces to the PSTN or PBX with either T1/CAS or T1/PRI interfaces. The following example shows debug output of commands such as debug voip ccapi inout, debug H225 events, and debug H225 asn1.

In the following debug output, the Cisco IOS Gateway accepts the TCP connection request from Cisco Unified CallManager (172.16.70.228) on port 2328 for H.225.

```
*Mar 12 04:03:57.169: H225Lib::h225TAccept: TCP connection accepted from
172.16.70.228:2328 on socket [1]
*Mar 12 04:03:57.169: H225Lib::h225TAccept: Q.931 Call State is initialized to be [Null].
*Mar 12 04:03:57.177: Hex representation of the received TPKT03000065080000100
```

The following debug output shows that the H.225 data is coming from the Cisco Unified CallManager 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 Cisco Unified CallManager.

```
*Mar 12 04:03:57.197: ccCallSetContext (callID=0x12, context=0x61466B30)
*Mar 12 04:03:57.197: ccCallProceeding (callID=0x11, prog_ind=0x0)
*Mar 12 04:03:57.197: cc_api_call_proceeding(vdbPtr=0x617BE064, callID=0x12, prog_ind=0x0)
*Mar 12 04:03:57.197: cc_api_call_alert(vdbPtr=0x617BE064, callID=0x12, prog_ind=0x8,
sig_ind=0x1)
*Mar 12 04:03:57.201: sess_appl: ev(17=CC_EV_CALL_PROCEEDING), cid(18), disp(0)
*Mar 12 04:03:57.201: ssa:
cid(18)st(1)oldst(0)cfid(-1)csize(0)in(0)fDest(0)-cid2(17)st2(1)oldst2(0)
*Mar 12 04:03:57.201: ssaIgnore cid(18), st(1),oldst(1), ev(17)
*Mar 12 04:03:57.201: sess_appl: ev(7=CC_EV_CALL_ALERT), cid(18), disp(0)
*Mar 12 04:03:57.201: ssa:
cid(18)st(1)oldst(1)cfid(-1)csize(0)in(0)fDest(0)-cid2(17)st2(1)oldst2(0)
*Mar 12 04:03:57.201: ssaFlushPeerTagQueue cid(17) peer list: (empty)
*Mar 12 04:03:57.201: ccCallAlert (callID=0x11, prog_ind=0x8, sig_ind=0x1)
*Mar 12 04:03:57.201: ccConferenceCreate (confID=0x617A8808, callID1=0x11, callID2=0x12,
tag=0x0)
*Mar 12 04:03:57.201: cc_api_bridge_done (confID=0x7, srcIF=0x616C9F54, srcCallID=0x11,
dstCallID=0x12, disposition=0, tag=0x0)value H323-UserInformation
*Mar 12 04:03:57.201: {
```

```
*Mar 12 04:03:57.201:   h323-uu-pdu
*Mar 12 04:03:57.201:   {
*Mar 12 04:03:57.201:     h323-message-body alerting :
*Mar 12 04:03:57.201:       {
*Mar 12 04:03:57.201:         protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:57.205:         destinationInfo
*Mar 12 04:03:57.205:         {
*Mar 12 04:03:57.205:           mc FALSE,
*Mar 12 04:03:57.205:           undefinedNode FALSE
*Mar 12 04:03:57.205:         },
```

In this packet, Cisco IOS also sends the H.245 address and port number to Cisco Unified CallManager. Sometimes, the Cisco IOS Gateway will send the unreachable address, which could cause either no audio or one-way audio.

```
*Mar 12 04:03:57.205:         h245Address ipAddress :
*Mar 12 04:03:57.205:           {
*Mar 12 04:03:57.205:             ip 'AC1046E2'H,
*Mar 12 04:03:57.205:             port 011008
*Mar 12 04:03:57.205:           },
*Mar 12 04:03:57.213: Hex representation of the ALERTING TPKT to send.0300003D0100
*Mar 12 04:03:57.213:
*Mar 12 04:03:57.213:       H225Lib::h225AlertRequest: Q.931 ALERTING sent from socket
[1]. Call state changed to [Call Received].
*Mar 12 04:03:57.213: cc_api_bridge_done (confID=0x7, srcIF=0x617BE064, srcCallID=0x12,
dstCallID=0x11, disposition=0, tag=0x0)
```

The following debug output shows that the H.245 session is coming up. You can see the capability indication for codec negotiation, as well as how many bytes will be present in each voice packet.

```
*Mar 12 04:03:57.217: cc_api_caps_ind (dstVdbPtr=0x616C9F54, dstCallId=0x11,
srcCallId=0x12, caps={codec=0xEBFB, fax_rate=0x7F, vad=0x3, modem=0x617C5720
codec_bytes=0, signal_type=3})
*Mar 12 04:03:57.217: sess_appl: ev(23=CC_EV_CONF_CREATE_DONE), cid(17), disp(0)
*Mar 12 04:03:57.217: ssa:
cid(17)st(3)oldst(0)cfid(7)csize(0)in(1)fDest(1)-cid2(18)st2(3)oldst2(1)
*Mar 12 04:03:57.653: cc_api_caps_ind (dstVdbPtr=0x617BE064, dstCallId=0x12,
srcCallId=0x11, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
```

The following debug output shows that both parties negotiated correctly and agreed on G.711 codec with 160 bytes of data.

```
*Mar 12 04:03:57.653: cc_api_caps_ack (dstVdbPtr=0x617BE064, dstCallId=0x12,
srcCallId=0x11, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
*Mar 12 04:03:57.653: cc_api_caps_ind (dstVdbPtr=0x617BE064, dstCallId=0x12,
srcCallId=0x11, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x, codec_bytes=160,
signal_type=0})
*Mar 12 04:03:57.653: cc_api_caps_ack (dstVdbPtr=0x617BE064, dstCallId=0x12,
srcCallId=0x11, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
*Mar 12 04:03:57.657: cc_api_caps_ack (dstVdbPtr=0x616C9F54, dstCallId=0x11,
srcCallId=0x12, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
*Mar 12 04:03:57.657: cc_api_caps_ack (dstVdbPtr=0x616C9F54, dstCallId=0x11,
srcCallId=0x12, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
```

The H.323 connect and disconnect messages follow.

```
*Mar 12 04:03:59.373: cc_api_call_connected(vdbPtr=0x617BE064, callID=0x12)
*Mar 12 04:03:59.373: sess_appl: ev(8=CC_EV_CALL_CONNECTED), cid(18), disp(0)
```

```
*Mar 12 04:03:59.373: ssa:
cid(18)st(4)oldst(1)cfid(7)csize(0)in(0)fDest(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)
```

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/0:-36/-42 dBm
```

INDEX

D

E

F

O

P

R

S

T