



Cisco IPICS Troubleshooting Guide

Release 2.1(1)

Americas Headquarters

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

Customer Order Number:
Text Part Number: OL-12986-01

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

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

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

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

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

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

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

Cisco IPICS Troubleshooting Guide, Release 2.1(1)
© 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xi

Audience xi

Organization xii

Related Documentation xiii

Cisco Unified Communications Manager (CallManager) Documentation xiv

Cisco Unified Communications Manager Express Documentation xv

Cisco 7800 Series Media Convergence Servers Documentation xv

Cisco Unified IP Phones 7900 Series Documentation xv

Session Initiation Protocol Documentation xv

Cisco Land Mobile Radio over IP/Solution Reference Network Design xvi

Cisco Security Agent xvi

Cisco IOS Documentation xvi

Document Notes and Conventions xvi

Obtaining Documentation, Obtaining Support, and Security Guidelines xviii

CHAPTER 1

Finding Troubleshooting Information for Cisco IPICS 1-1

CHAPTER 2

Troubleshooting Cisco IPICS Network Processes 2-1

Performing Tomcat Service Procedures 2-2

Checking the Status of the Tomcat Service 2-2

Manually Stopping the Tomcat Service 2-3

Manually Starting the Tomcat Service 2-5

Manually Restarting the Tomcat Service 2-6

Performing Database Server Procedures 2-6

Checking the Status of the Database Server 2-7

| | |
|--|------|
| Manually Restarting the Database Server | 2-8 |
| Manually Starting the Database Server | 2-9 |
| Performing License Manager Procedures | 2-9 |
| Checking the Status of the License Manager | 2-10 |
| Restarting the License Manager | 2-11 |
| Manually Starting the License Manager | 2-12 |
| Performing Dial Engine Procedures | 2-12 |
| Checking the Status of the Dial Engine | 2-13 |
| Manually Stopping the Dial Engine | 2-14 |
| Manually Restarting the Dial Engine | 2-14 |
| Manually Starting the Dial Engine | 2-15 |
| Performing CSA Procedures | 2-16 |
| Viewing CSA Log Messages | 2-17 |
| Manually Stopping CSA | 2-18 |
| Manually Starting CSA | 2-18 |

CHAPTER 3

Troubleshooting the Cisco IPICS Server 3-1

| | |
|--|------|
| Troubleshooting Cisco IPICS Installation Issues | 3-1 |
| Troubleshooting Cisco IPICS Administration Console Issues | 3-2 |
| Resolving Intermittent Browser Problems | 3-3 |
| Resolving Failures to Access the Server With an Administration Console Browser Session | 3-4 |
| Enlarging the Text in the Administration Console | 3-9 |
| Reducing Text in the Administration Console | 3-9 |
| Analyzing 404 or 500 Error Messages When You Attempt to Access the Administration Console | 3-10 |
| Troubleshooting Browser Timeout Issues When You Configure an RMS with Twelve or More Loopback Interfaces | 3-12 |
| Performing Database Procedures To Resolve Login Problems and Failure To Complete Tasks in the Administration Console | 3-14 |

| | |
|--|------|
| VTG Activates Without Dispatcher Action | 3-15 |
| Troubleshooting VTG Activation Problems | 3-16 |
| VTG Does Not Appear on User PMC | 3-17 |
| Troubleshooting an Ops View Save Failure | 3-17 |
| Resolving Administration Console Undefined Errors | 3-19 |
| Commands Fail Intermittently | 3-20 |
| Adding Fonts to Internet Explorer to Fix Language Character Display Problems | 3-20 |
| PMC Users Receive Error Messages During Login After a Database Restore Operation | 3-21 |
| Configuration Changes Do Not Get Saved When Multiple Users Configure Cisco IPICS | 3-22 |
| Recovering a Deleted System Administrator User | 3-23 |
| Troubleshooting User ID and Password Issues | 3-24 |
| Resetting a Forgotten or Missing ipics User Password | 3-24 |
| Resetting the Password for the ipicsadmin or informix User ID | 3-24 |
| Changing the root User Password | 3-25 |
| Resetting a Locked or Disabled User Account | 3-26 |
| Troubleshooting License Issues | 3-27 |
| Resolving Invalid Base Server License Messages that Display After You Upload the License File | 3-27 |
| After Uploading Multiple License Files, All Features Do Not Display in the Administration Console | 3-31 |
| After Changing the Server IP Address, You Experience Host Name Mismatch or Problems Installing the License | 3-32 |
| Changing System Date Invalidates Time-Bound License | 3-32 |
| Suppressing Server Expiration Messages After Installing a More Recent Time-Bound License | 3-33 |
| Troubleshooting Policy Engine Issues | 3-34 |
| Uploading a Large Zipped File of Prompts Causes an Error | 3-35 |
| IppeAgentImpl ERROR Messages Display in the ipics.log File | 3-36 |

| | |
|--|------|
| Resolving Communication Problems Between the Policy Engine and the Prompt Manager | 3-38 |
| Resolving Reconnection Failures After a Dial-In Caller Uses the Hold or Call Waiting Feature | 3-38 |
| Troubleshooting Dial-In Call Connection Failures | 3-39 |
| Troubleshooting Dial-Out Invitation Failures | 3-43 |
| Troubleshooting Dial-Out Notification Failures | 3-44 |
| Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views | 3-46 |
| Understanding a PARTIAL_SERVICE Status For the Dial Engine and Subsystem Manager | 3-46 |
| Analyzing a SHUTDOWN Status For the SIP Subsystem | 3-47 |

CHAPTER 4

Troubleshooting Communication, Voice Quality and Other Equipment Issues 4-1

| | |
|---|-----|
| Troubleshooting Communication Issues | 4-1 |
| Analyzing Communications Problems Between All Locations on a Channel | 4-2 |
| Troubleshooting Communication Failures Between VTG Participants | 4-2 |
| Resolving Communications Problems For Newly-Added PMC Users on a Channel | 4-3 |
| Removing a Logged-Out PMC User from the Active Users List | 4-4 |
| PMC Users Can Listen to Channels But Cannot Listen to VTGs | 4-4 |
| Configuring the RMS to Eliminate Automatic Channel Deactivation for SIP-Based Remote Connections | 4-5 |
| Eliminating Feedback Noise on VTG | 4-6 |
| Understanding Communication Problems Between Cisco IPICS End Point Devices and Radios That Require a Guard Tone | 4-6 |
| Troubleshooting Voice Quality Issues | 4-7 |
| Voice Quality Degrades for PMC | 4-8 |
| Troubleshooting Poor PMC Voice Quality | 4-8 |
| Dial Engine Calls Experience Degraded Voice Quality | 4-9 |

| | |
|--|------|
| Resolving Interruption of Voice Communications When You Use VTGs and SIP-Connected PMC Client Machines | 4-9 |
| Troubleshooting Equipment Issues | 4-10 |
| No Power to Cisco Unified IP Phones | 4-11 |
| Analyzing One-Way Audio Issues Between PMC Client Machines and Cisco Unified IP Phones | 4-12 |
| Resolving One-Way Audio Problems on the Cisco Unified IP Phone That Occurs After You Receive or Place a Call | 4-12 |
| Correcting Channel Accessibility Issues with Cisco Unified IP Phones | 4-13 |
| Cisco Unified IP Phone Cannot Access the Cisco IPICS Service After Changing the Server IP Address | 4-13 |
| Resolving Interconnectivity Problems With Cisco Unified Wireless IP Phone 7920 | 4-14 |
| Cisco MCS 7825-H2 Server Becomes Inoperable After Removing the Second Hard Drive | 4-15 |
| Troubleshooting RMS Configuration Issues | 4-15 |
| Server Reboots Slowly Following RMS Configuration | 4-16 |
| You Attempt to Deactivate an RMS but its Status Does Not Change | 4-16 |
| VTG Activation Slow or RMS in Unreachable State After RMS Command Prompt Changed | 4-18 |
| RMS Fails or Remains in Unreachable State | 4-18 |
| Newly-Added RMS Does Not Display Loopbacks | 4-19 |
| Router Remains in Unreachable State | 4-19 |
| The Cisco IPICS Server Does Not Recognize All of the T1 Ports on the RMS | 4-20 |
| Router Indicator Lights for the Loopback Are Not Green | 4-21 |
| Voice Loops in VTGs and Router Configuration Shows Incorrect Information | 4-22 |
| Long Delays Between Pressing the PMC PTT Button and Media Establishment | 4-24 |

CHAPTER 5**Troubleshooting Tips for the PMC Application 5-1**

Troubleshooting PMC Application Problems 5-1

Resolving PMC Execution Issues 5-2

Generating a PMC Installation Log File 5-3

Using the PMC Installer with an Encrypted File System 5-5

Making PMC Configuration File Changes 5-6

Using the PMC Optional Settings 5-6

Resolving Footswitch/USB Device Issues 5-7

Configuring the Audio Settings 5-7

Using a USB DSP Headset with the PMC 5-8

Checking the Microphone with the PMC 5-9

Using Cisco Security Agent with the PMC 5-9

PMC Coexistence with Other Voice Applications 5-10

Troubleshooting One-Way Audio 5-11

Using CLI Commands to Resolve Audio and Headset Issues 5-11

Resolving IP Address Changes 5-13

Troubleshooting Voice Quality Issues 5-14

Resolving Unknown Publisher Errors with Windows XP SP2 5-15

Resolving Cisco IPICS Server Administration Console Access Issues with Internet Explorer 5-15

Troubleshooting PMC Connectivity Issues 5-16

Troubleshooting VPN Connectivity 5-16

Using the PMC with the Windows XP Firewall 5-19

Resolving Issues with the Microsoft QoS Packet Scheduler 5-20

Troubleshooting Multicast Communications Issues 5-21

Troubleshooting Winsock Corruption Issues 5-22

Troubleshooting Offline Mode Issues 5-23

Troubleshooting PMC Connectivity Issues with the RMS 5-24

Troubleshooting PMC Connectivity Issues with a High Latency, Low Bandwidth Link 5-25

| | |
|---|------|
| Resolving Name Resolution Failures | 5-25 |
| Identifying Channel Activation Issues | 5-26 |
| Resolving Codec Mismatch Issues | 5-27 |
| Support for Right-to-Left and Double-Byte Languages | 5-27 |
| PMC Application Caveats | 5-29 |
| Analyzing PMC Error Conditions | 5-30 |

CHAPTER 6**Using the Cisco IPICS CLI Tools and Service Commands 6-1**

| | |
|--|-----|
| Understanding the CLI-based Tools | 6-1 |
| Using the CLI-based Tools | 6-2 |
| Unlocking or Enabling a Locked or Disabled User With the enableuser Tool | 6-3 |
| Changing the Server IP Address With the modify_ip Tool | 6-4 |
| Configuring NTP on the Cisco IPICS Server with the ntpsetup Tool | 6-5 |
| ntpsetup Command Examples | 6-7 |
| Resetting, Changing, or Creating a Password With the reset_pw Tool | 6-7 |
| Configuring and Checking Cisco IPICS Network Processes With Service Commands | 6-9 |

CHAPTER 7**Understanding the Cisco IPICS Logs 7-1**

| | |
|--|------|
| Understanding and Locating the Cisco IPICS Log Files | 7-1 |
| Generating and Modifying the PMC Log Levels | 7-7 |
| Understanding PMC Debug Log Information | 7-9 |
| Using the Debugging Log Level | 7-10 |
| Checking CSA Logs | 7-15 |
| Viewing the CSA Messages from the CSA Utility | 7-16 |
| Opening the CSA Security Event Log with CLI Commands | 7-16 |

GLOSSARY

INDEX



Preface

The Cisco IPICS Troubleshooting Guide, Release 2.1(1) provides you with the information that you need to troubleshoot problems that you may encounter when you install, configure, or use the Cisco IP Interoperability and Collaboration System (hereafter referred to as *Cisco IPICS*) solution. System administrators should review this document to aid in their troubleshooting efforts for problems that they may encounter when they use Cisco IPICS.

Audience

The *Cisco IPICS Troubleshooting Guide, Release 2.1(1)* targets system administrators who install, configure, operate, and manage tasks on the Cisco IPICS system. This document also targets end users who communicate with other users by using the Cisco IPICS Push-to-Talk Management Center (PMC) application or Cisco Unified IP Phone.

Organization

This document is organized as follows:

| | |
|--|--|
| Chapter 1, “Finding Troubleshooting Information for Cisco IPICS” | This chapter provides information about how to find troubleshooting information for Cisco IPICS. |
| Chapter 2, “Troubleshooting Cisco IPICS Network Processes” | This chapter includes troubleshooting tips for the network processes that the Cisco IPICS server uses, such as the tomcat service, the database server, the license manager, the dial engine, and the Cisco Security Agent (CSA). |
| Chapter 3, “Troubleshooting the Cisco IPICS Server” | This chapter includes information about troubleshooting the Cisco IPICS server and Cisco IPICS policy engine (hereafter known as policy engine). It also includes information about components that work with Cisco IPICS, such as Cisco Unified IP Phones and the router media service (RMS). |
| Chapter 4, “Troubleshooting Communication, Voice Quality and Other Equipment Issues” | This chapter describes how to resolve communications and voice quality issues and hardware, firmware, and software issues that you might encounter with non-server equipment, such as the RMS. |
| Chapter 5, “Troubleshooting Tips for the PMC Application” | This chapter includes troubleshooting information for the PMC. |
| Chapter 6, “Using the Cisco IPICS CLI Tools and Service Commands” | This chapter includes information about the command line interface (CLI) tools and service commands that you can use with Cisco IPICS. |
| Chapter 7, “Understanding the Cisco IPICS Logs” | This chapter includes information about the activity and error logs that Cisco IPICS generates, along with information about how to interpret the data in the logs. |

Related Documentation

For more information about Cisco IPICS and the PMC application, refer to the following documentation:

- *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*—This document describes how to install, configure, manage, and operate the Cisco IPICS PMC application.
- *Cisco IPICS PMC Quick Start Reference Card, Release 2.1(1)*—This document provides tips and quick references for the most frequently used procedures that a user can perform on the Cisco IPICS PMC.
- *Cisco IPICS PMC Debug Reference Quick Start Card, Release 2.1(1)*—This document provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC.
- *Cisco IPICS PMC Command Line Interface, Release 2.1(1)*—This document describes the commands that you can use from the command line interface (CLI) to obtain information or to change settings for the Cisco IPICS PMC.
- *Cisco IPICS Server Administration Guide, Release 2.1(1)*—This document contains information about the key configuration, operation, and management tasks for the Cisco IPICS server.
- *Cisco IPICS Server Quick Start Guide, Release 2.1(1)*—This document is a condensed version of the *Cisco IPICS Server Administration Guide* to help the administrator to quickly get started with Cisco IPICS.
- *Cisco IPICS Server Quick Start Reference Card, Release 2.1(1)*—This document provides tips, quick references, and usage guidelines for the Cisco IPICS server.
- *Using Cisco IPICS on Your IP Phone Quick Start Reference Card, Release 2.1(1)*—This document contains information about accessing Cisco IPICS from your IP phone and tips and guidelines for using this service.
- *Using the Cisco IPICS TUI Quick Start Reference Card, Release 2.1(1)*—This document describes the steps that you follow to dial in to, or receive a call from, the policy engine telephony user interface (TUI) and guidelines for using the system.

- *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card, Release 2.1(1)*—This document contains examples of valid and invalid radio control and signaling descriptor file entries and guidelines for creating these entries.
- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*—This document describes how to install, configure, and upgrade the Cisco IPICS server software and Cisco IPICS operating system.
- *Cisco IPICS Server Quick Start Installation Reference Card, Release 2.1(1)*—This document provides tips and quick references for installing and upgrading the Cisco IPICS server.
- *Release Notes for Cisco IPICS Release 2.1(1)*—This document contains a description of the new and changed features, important notes, caveats, and documentation updates for this release of Cisco IPICS.
- *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.1(1)*— This document provides information about design considerations and guidelines for deploying the Cisco IPICS solution.
- *Cisco IPICS Compatibility Matrix*—This document contains information about compatible hardware and software that is supported for use with Cisco IPICS.
- *Cisco IPICS 2.1(1) Resources Card (Documentation Locator)*—This document provides a summary of the documentation that is available for this release of Cisco IPICS.

To access the documentation suite for Cisco IPICS, refer to the following URL:

http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

Cisco Unified Communications Manager (CallManager) Documentation

For information about Cisco Unified Communications Manager (CallManager), refer to the documentation at this URL:

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

Cisco Unified Communications Manager Express Documentation

For information about Cisco Unified Communications Manager Express, refer to the documentation at this URL:

http://cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_home.html

Cisco 7800 Series Media Convergence Servers Documentation

For information about Cisco 7800 Series Media Convergence Servers, refer to the MCS data sheets at this URL:

http://www.cisco.com/en/US/products/hw/voiceapp/ps378/products_data_sheets_list.html

Cisco Unified IP Phones 7900 Series Documentation

For information about Cisco Unified IP Phones, refer to the documentation at this URL:

http://cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

Session Initiation Protocol Documentation

The dial engine, which controls the dial-in and dial-out functionality of the policy engine, uses the Session Initiation Protocol (SIP). For information about SIP, refer to the documentation at this URL:

http://cisco.com/en/US/tech/tk652/tk701/tk587/tsd_technology_support_sub-protocol_home.html

Cisco Land Mobile Radio over IP/Solution Reference Network Design

For information about Cisco Land Mobile Radio (LMR) over IP, refer to the documentation at the following URLs:

- http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00801f092c.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_implementation_design_guide_book09186a0080347c1b.html

Cisco Security Agent

For information about Cisco Security Agent, refer to the documentation at this URL:

<http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html>

Cisco IOS Documentation

The Cisco IOS software documentation set describes the tasks and commands necessary to configure certain system components and other Cisco products, such as access servers, routers, and switches. Each configuration guide can be used in conjunction with its corresponding command reference.

For information about Cisco IOS software configuration, refer to the documentation at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html

Document Notes and Conventions

This document uses the following conventions for instructions and information:

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

**Caution**

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

Table 1 **Conventions**

| Convention | Description |
|------------------------------------|---|
| boldface font | Commands and keywords appear in boldface . |
| <i>italic font</i> | Command input for which you supply the values appear in <i>italics</i> . |
| [] | Optional keywords and default responses to system prompts appear within square brackets. |
| { x x x } | A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| ^ or Ctrl | Represent the key labeled <i>Control</i> . For example, when you read ^D or <i>Ctrl-D</i> , you should hold down the Control key while you press the D key. |
| screen font | Examples of information displayed on the screen. |
| boldface screen font | Information that you must enter is in boldface screen font . |
| <i>italic screen font</i> | Arguments for which you supply values are in <i>italic screen font</i> . |

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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



CHAPTER 1

Finding Troubleshooting Information for Cisco IPICS

This chapter provides information about how to find troubleshooting information for Cisco IPICS. See [Table 1-1](#) for links that pertain to available troubleshooting information for problems that you may encounter.

Table 1-1 ***Locating Troubleshooting Information***

| Source of Problem | Where to Find Help |
|---|--|
| Cisco IPICS installation | To troubleshoot problems that are related to the Cisco IPICS installation, refer to the “Troubleshooting the Installation” chapter of the Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1) . |
| One of the following areas: <ul style="list-style-type: none">• The Cisco IPICS server• Policy engine• Communications between Cisco IPICS end-user devices• Equipment, such as Cisco Unified IP Phones or radios• RMS configuration• General operation | For problems that are related to the server, the policy engine, and the devices that communicate with the server, see Chapter 3, “Troubleshooting the Cisco IPICS Server.” For help in gathering log information to aid your problem determination and resolution process, see Chapter 7, “Understanding the Cisco IPICS Logs.” |

Table 1-1 **Locating Troubleshooting Information (continued)**

| Source of Problem | Where to Find Help |
|---|--|
| <p>One of the following areas:</p> <ul style="list-style-type: none"> • Communications between Cisco IPICS endpoints • Hardware, such as Cisco Unified IP Phones • Router and RMS configuration • Voice quality | <p>For communications-related problems, problems with endpoint devices, and voice quality issues, see Chapter 4, “Troubleshooting Communication, Voice Quality and Other Equipment Issues.”</p> |
| PMC issues | <p>To troubleshoot problems that you may encounter when you install or use the PMC application, see Chapter 5, “Troubleshooting Tips for the PMC Application.”</p> <p>For help in gathering PMC log information to aid your problem determination and resolution process, see the “Generating and Modifying the PMC Log Levels” section on page 7-7.</p> |
| Backup and restore | <p>To obtain information about backing up or restoring the Cisco IPICS database, or to troubleshoot problems that you encounter in the backup or restore process, refer to the “Performing Cisco IPICS Database Backup and Restore Operations” chapter in the Cisco IPICS Server Administration Guide, Release 2.1(1).</p> |
| License | <p>For information about problems that are related to the installation and usage of licenses, see the “Troubleshooting License Issues” section on page 3-27.</p> |



CHAPTER 2

Troubleshooting Cisco IPICS Network Processes

When you boot up the Cisco IPICS server, the server software automatically starts the following network processes:

- Tomcat service
- Database server
- License manager
- Dial engine (if the policy engine is licensed for your server)
- Cisco Security Agent (CSA)

This chapter provides information to help you to troubleshoot these processes and includes the following sections:

- [Performing Tomcat Service Procedures, page 2-2](#)
- [Performing Database Server Procedures, page 2-6](#)
- [Performing License Manager Procedures, page 2-9](#)
- [Performing Dial Engine Procedures, page 2-12](#)
- [Performing CSA Procedures, page 2-16](#)

**Note**

This chapter documents procedures that use command-line interface (CLI) commands. If the tomcat service and database server are both running, you can check their status without using CLI by logging in to the Administration Console, navigating to the **Serviceability > Diagnostics** window, and viewing the information in the Diagnostic Summary pane.

Performing Tomcat Service Procedures

The tomcat service contains all of the Cisco IPICS web-based applications. The tomcat service runs processes that are required for the functional operation of Cisco IPICS, and must run continuously for you to access the Administration Console and other web applications.

Cisco IPICS includes a cron job that acts as a safeguard to make sure that the tomcat service continues to run. This cron job checks the status of the tomcat service every 60 seconds and can restart the service automatically, if the tomcat service stops.

This section includes information about the tomcat service in the following topics:

- [Checking the Status of the Tomcat Service, page 2-2](#)
- [Manually Stopping the Tomcat Service, page 2-3](#)
- [Manually Starting the Tomcat Service, page 2-5](#)
- [Manually Restarting the Tomcat Service, page 2-6](#)

Checking the Status of the Tomcat Service

You can check the status of the tomcat service by navigating to the **Serviceability > Diagnostics** window of the Administration Console and viewing the Cisco IPICS Tomcat Web Server Status field.

If the tomcat service or the database server is not running, you cannot check its status in the Administration Console. In this case, you must enter CLI commands to check its status. To check the status of the tomcat service by using CLI commands, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 Check the status of the tomcat service by entering the following command:

```
[root]# service ipics_tomcat status
```

If the tomcat service is running properly, the command returns a process similar to the following example:

```
Tomcat process (pid: 24025) is running on the system
```

If the tomcat service is not running, you should see a response that is similar to the following example:

```
Tomcat is not running on the system.
```

If the tomcat service is not running, you can start it manually by entering the **service ipics_tomcat start** CLI command from the root user ID. For more information, see the [“Manually Starting the Tomcat Service” section on page 2-5](#).

Manually Stopping the Tomcat Service

If you do not want any users to access the Administration Console when you perform system maintenance tasks, such as database-related activities, you can stop the tomcat service.

To stop the tomcat service, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

The terminal console displays.

Step 2 To stop the tomcat service, enter the following command:

```
[root]# service ipics_tomcat stop
```

If the tomcat service stops, Cisco IPICS displays the message [OK].

If the tomcat service does not stop, an error message displays that indicates that Cisco IPICS cannot stop the service; if you receive this message, continue to [Step 3](#).

Step 3 If the tomcat service fails to stop, you can terminate the processes that are running by performing the following procedure:

- a. To check which tomcat processes are still running, enter the following `grep` command, which returns information about the tomcat processes that continue to run:

```
[root]# ps -ef | grep tomcat
```

This command shows you a list of the running tomcat processes.

- b. Note the Process IDs, which display in the second column of the `grep` results.
- c. To stop the tomcat processes that are still running, enter the following command:

```
[root]# kill -9 <process-id>
```

where:

<process-id> specifies the Process IDs that you noted in [Step b](#).

- d. Repeat [Step c](#) for every tomcat process that is running.

Step 4 Check the status of the tomcat service by entering the following command:

```
[root]# service ipics_tomcat status
```

If the tomcat service stops successfully, the following message displays:

```
Tomcat is not running on the system.
```

Step 5 If the tomcat service does not stop, check the `ipics.log` file to gather information on the nature of the problem by entering the following command:

```
[root]# tail -75 /root/tomcat/current/logs/ipics.log
```



Note

The `ipics.log` file contains messages regarding all transactions that occur in the Cisco IPICS server, including tomcat service transactions.

The last 75 lines of the `ipics.log` file displays.

Step 6 Attempt to fix the problem based on the information that you view in the log file.

The information might include information about a running process that could not stop.

- Step 7** If you cannot resolve the problem by using the information in the ipics.log file, contact your Cisco technical support representative for further assistance.
-

Manually Starting the Tomcat Service

If the cron job fails to start the tomcat service successfully, or if you stop the tomcat service, you can start the service manually by using CLI commands.

To manually start the tomcat service, perform the following procedure:

Procedure

- Step 1** Log in to the Cisco IPICS server by using the root user ID.

A terminal window displays.

- Step 2** To start the tomcat service, enter the following command:

```
[root]# service ipics_tomcat start
```

If the tomcat service starts successfully, Cisco IPICS displays the message [OK].



Note After you start the tomcat service, there may be a delay of a few minutes before users can access the Administration Console.

- Step 3** If the tomcat service does not successfully start, check the ipics.log file to gather information on the nature of the problem by entering the following command:

```
[root]# tail -75 /root/tomcat/current/logs/ipics.log
```



Note The ipics.log file contains messages regarding all transactions that occur in the Cisco IPICS server, including tomcat service transactions.

The last 75 lines of the ipics.log file displays.

- Step 4** Attempt to fix the problem based on the information that you view in the log file.

The information might contain a Java exception error or provide information about a process that did not start.

- Step 5** If you cannot resolve the problem by using the information in the ipics.log file, contact your Cisco technical support representative for further assistance.
-

Manually Restarting the Tomcat Service

To restart the tomcat service, perform the following procedure:



Note When you restart the tomcat service, the script logs out any users who are logged in to the Administration Console.

Procedure

- Step 1** Log in to the Cisco IPICS server by using the root user ID.

- Step 2** To restart the tomcat service, enter the following command:

```
[root]# service ipics_tomcat restart
```

After restarting the tomcat service, Cisco IPICS displays the message [OK].



Note After you start the tomcat service, there may be a delay of a few minutes before users can access the Administration Console.

Performing Database Server Procedures

The database server performs all database-related activities in Cisco IPICS, such as backup and restore operations and database updates.

This section includes the procedures to start, stop, and check the status of the database server in the following topics:

- [Checking the Status of the Database Server, page 2-7](#)
- [Manually Restarting the Database Server, page 2-8](#)
- [Manually Starting the Database Server, page 2-9](#)

Checking the Status of the Database Server

You can check the status of the database server via the Administration Console. To do so, navigate to the **Serviceability > Diagnostics** window and view the Diagnostic Summary area. Navigate to the Cisco IPICS Database Status area in this pane to view the database server status.

If the database server is stopped, you cannot log in to the Administration Console to check its status; however, you can check the status of the database server by entering CLI commands. To check the status of the database server, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To check the status of the database server, enter the following command:

```
[root]# service ipics_db status
```

If the database server is running properly, the server displays a message that is similar to the following example:

```
Ipics Database is running...
oninit (pid 21286 21285 21284 21283 21282 21281 21280) is running...
```

If the database server is not running, the server displays a message that is similar to the following example:

```
Ipics Database is stopped.
```

If the database server is not running, you can manually start the database server by performing the procedure in the [“Manually Starting the Database Server” section on page 2-9](#).

Manually Restarting the Database Server

If you experience Cisco IPICS server performance issues, determine whether the database server is the cause of the problem by checking the system resources that the database is using. To check system resources, perform one of the following actions:

- From the Administration Console, navigate to the **Serviceability > Dashboard** window and check the memory information that is displayed in the System Dashboard area.
- Log in to a terminal console session by using the root user ID; then, enter the **top** command.



Note The **top** command displays a listing of the server processes that are using the greatest amount of CPU memory.

If you determine that the Cisco IPICS processes are using a large amount of memory, you can restart the database server, which might speed up network processes.

To restart the database server, perform the following procedure:

Procedure

-
- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** To restart the database server, enter the following command:
- ```
[root]# service ipics_db restart
```
- Cisco IPICS displays the message [OK] when the database server successfully stops and displays the message [OK] again when the database server successfully restarts.
- Step 3** If you receive an error message after you attempt to restart the database server, contact your Cisco technical support representative for further assistance.
-

## Manually Starting the Database Server

Cisco IPICS starts the database server when the server boots up. You can also start the database server manually if you determine that the database has stopped. To check whether the database is running, see the [“Checking the Status of the Database Server” section on page 2-7](#).

To manually start the database server from a terminal console session, perform the following procedure:

### Procedure

- 
- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** To start the database server, enter the following command:
- ```
[root]# service ipics_db start
```
- If the database server starts successfully, Cisco IPICS displays the message [OK].
- Step 3** If the database does not successfully start, contact your Cisco technical support representative for further assistance.



Tip To check the log file for the database, enter the following command:

```
[root]# more /opt/cisco/ipics/database/logs/diagnostics.log
```

The diagnostics.log file might provide you with additional details about the reason that the database could not start. Messages such as “Assert failed” or “PANIC” indicate a problem with the database that requires the assistance of your Cisco technical support representative.

Performing License Manager Procedures

The license manager is the network process that manages the Cisco IPICS licenses.

The license manager checks for new licenses every 24 hours. For a new license file to take effect immediately, you must restart the license manager.

This section includes the procedures to start, stop, and check the status of the license manager and includes the following topics:

- [Checking the Status of the License Manager, page 2-10](#)
- [Restarting the License Manager, page 2-11](#)
- [Manually Starting the License Manager, page 2-12](#)

Checking the Status of the License Manager

To check the status of the license manager from the Cisco IPICS Administration Console, navigate to the **Serviceability > Diagnostics** window and view the Diagnostic Summary area. Navigate to the Cisco IPICS Tomcat Web Server Status area in this pane to view the license manager status.



Tip

Any field that includes the words **lmgrd** contains information about the license manager.

To manually check the status of the license manager, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To check the status of the license manager, enter the following command:

```
[root]# service ipics_lm status
```

If the license manager is running, the server displays a message that is similar to the following example:

```
ipics_lm is running (PID 20859).
```

If the license manager is not running, the server displays a message that is similar to the following example:

```
ipics_lm is not running.
```

- Step 3** If the license manager is not running, you can manually start the license manager by following the procedure in the [“Manually Starting the License Manager” section on page 2-121](#).
-

Restarting the License Manager

If you add files, or change the system date, you must restart the license manager for the license and date changes to take effect.

To restart the license manager from the Administration Console, navigate to the **Administration > License Management** window and click the **Apply** button.

To restart the license manager by using CLI commands, perform the following procedure:

Procedure

- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** To restart the license manager, enter the following command:
- ```
[root]# service ipics_lm restart
```
- Cisco IPICS displays the message [OK] when the license manager successfully stops and displays the message [OK] again when the license manager successfully restarts.
- Step 3** If you receive an error message that indicates that the license manager or lmgrd process could not start, contact your Cisco technical support representative for further assistance.
-

## Manually Starting the License Manager

If the license manager has stopped, you should be able to restart it from the Administration Console by navigating to the **Administration > License Management** window and clicking the **Apply** button. You can also manually start the license manager from a terminal console session by performing the following procedure:

### Procedure

---

- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** To start the license manager, enter the following command:
- ```
[root]# service ipics_lm start
```
- If the license manager starts successfully, Cisco IPICS displays the message `[OK]`.
- Step 3** If the license manager does not start, check the status by performing the actions that are documented in the [“Checking the Status of the License Manager” section on page 2-10](#).
- Step 4** If you cannot start the license manager, contact your Cisco technical support representative for further assistance.
-

Performing Dial Engine Procedures

The dial engine controls the dial-in and dial-out functionality for the policy engine. For more information about the policy engine and dial engine, refer to the “Using the Cisco IPICS Policy Engine” chapter in the [Cisco IPICS Server Administration Guide, Release 2.1\(1\)](#).



Note

Your Cisco IPICS system must be licensed for the policy engine before you can perform dial engine procedures. To check whether you are licensed for the policy engine, navigate to the **Administration > License Management > Summary** tab in the Administration Console and check the Policy Engine Base License field. If your system is licensed for the policy engine, the field displays a status of

Licensed. For more information about licenses, refer to the “Performing Cisco IPICS System Administrator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

This section provides information about starting, stopping, restarting and checking the status of the dial engine and includes the following topics:

- [Checking the Status of the Dial Engine, page 2-13](#)
- [Manually Stopping the Dial Engine, page 2-14](#)
- [Manually Restarting the Dial Engine, page 2-14](#)
- [Manually Starting the Dial Engine, page 2-15](#)

Checking the Status of the Dial Engine

To check the status of the dial engine, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To check the status of the dial engine, enter the following command:

```
[root]# service ippe_dial_engine status
```

If the dial engine is running properly, the server displays a message that is similar to the following example:

```
Checking status...
CVD process (pid 11290) is running...
Engine process (pid 11670) is running...
```

If the dial engine processes are not running, the server displays a message that is similar to the following example:

```
Checking status...
CVD process is NOT running...
Engine process is NOT running...
```

- Step 3** If the dial engine is not running, you can manually start the dial engine by performing the procedure in the [“Manually Starting the Dial Engine”](#) section on [page 2-15](#).
-

Manually Stopping the Dial Engine

To stop the dial engine by using CLI commands, perform the following procedure:

**Note**

Cisco IPICS disconnects all active dial-in and dial-out calls when you stop the dial engine.

Procedure

-
- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** To stop the dial engine, enter the following command:
- ```
[root]# service ippe_dial_engine stop
```
- Cisco IPICS displays the message [OK] when the dial engine processes successfully stop.
- 

## Manually Restarting the Dial Engine

To restart the dial engine by using CLI commands, perform the following procedure:

**Note**

Cisco IPICS disconnects all active dial-in and dial-out calls when you restart the dial engine.

---

**Procedure**

- 
- Step 1** Log in to the Cisco IPICS server by using the root user ID.

**Step 2** To restart the dial engine, enter the following command:

```
[root]# service ippe_dial_engine restart
```

Cisco IPICS displays the message [OK] when the dial engine processes stop and restart.

**Step 3** If you cannot restart the dial engine, perform the following steps:

- a. Check that the policy engine is licensed by navigating to the **Administration > License Management > Summary** tab.
- b. Check the status of your license in the Policy Engine Base License field.  
The status displays as Licensed or Not Licensed.
- c. Perform one of the following actions based on the output that displays:
  - If the Policy Engine Base License field shows a status of Not Licensed, you are not licensed for the policy engine. To purchase a license that includes policy engine functionality, refer to the “Obtaining Your License File” section in the “Installing Cisco IPICS” chapter in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.
  - If the Policy Engine Base License field shows a status of Licensed, contact your Cisco technical support representative for further assistance.

## Manually Starting the Dial Engine

If the dial engine has stopped, you can manually start it by using CLI commands by performing the following procedure:

### Procedure

**Step 1** Log in to the Cisco IPICS server by using the root user ID.

**Step 2** To start the dial engine, enter the following command:

```
[root]# service ippe_dial_engine start
```

If the dial engine processes starts successfully, Cisco IPICS displays the message [OK].

- Step 3** If you cannot start the dial engine, perform the following steps:
- a. Check that the policy engine is licensed by navigating to the **Administration > License Management > Summary** tab.
  - b. Check the status of your license in the Policy Engine Base License field. The status displays as Licensed or Not Licensed.
  - c. Perform one of the following actions based on the output that displays:
    - If the Policy Engine Base License field shows a status of Not Licensed, you are not licensed for the policy engine. To purchase a license and obtain dial engine and policy engine functionality, refer to the “Obtaining Your License File” “Installing Cisco IPICS” chapter of the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.
    - If the Policy Engine Base License field shows a status of Licensed, contact your Cisco technical support representative for further assistance.
- 

## Performing CSA Procedures

CSA provides threat protection for server and desktop computing systems. It also prevents users from performing unauthorized actions on the server. There may be times where stopping CSA is necessary to perform system-level functions, to debug an issue, or to edit protected system files.

This section describes how to perform certain CSA procedures and includes the following topics:

- [Viewing CSA Log Messages, page 2-17](#)
- [Manually Stopping CSA, page 2-18](#)
- [Manually Starting CSA, page 2-18](#)

## Viewing CSA Log Messages

If CSA denies a particular action, such as when a user or process attempts to modify or delete a protected file, the process generates a message similar to the following example:

```
Oct 15 04:02:02 [hostname] CiscoSecurityAgent[3480]: Event: The
process '/bin/cp' (as user root(0) group root(0)) attempted to access
'/var/cache/man/whatis'. The attempted access was an open. The
operation was denied.
```

You can view the CSA actions in the Security Event Log. To view the Security Event Log, perform the following procedure:

### Procedure

- 
- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** Navigate to the **/var/log** directory on the Cisco IPICS server by entering the following command:
- ```
[root]# cd /var/log
```
- Step 3** To list the files that start with the **csalog** name in the directory, enter the following command:
- ```
[root]# ls -l csa*og*
```
- All files that begin with **csalog** display.



#### Note

The Security Event Log file is named **csalog**. If the **csalog** file has reached its maximum size, Cisco IPICS creates a new file called **csalog.0**, copies the information in the **csalog** file to the **csalog.0** file, and removes the data in the **csalog** file. If the **csalog** file again reaches its maximum size, Cisco IPICS renames the **csalog.0** file to **csalog.1**, copies the information in the **csalog** file to the **csalog.0** file, and removes the data in the **csalog** file.

- Step 4** To view the log file, enter the following command:
- ```
[root]# cat csa*og.x
```
- where:
- x* is the numeric extension of the file (if applicable).

A text viewer window displays the contents of the Security Event Log. This log provides a detailed list of security events that CSA has detected and the action, if any, that CSA performed as a result of those events.

Manually Stopping CSA

You can stop CSA by issuing a command in a terminal console session. To stop CSA from a terminal console session, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To stop CSA, enter the following command:

```
[root]# service ciscosec stop
```

Cisco IPICS displays the message [OK] after CSA stops.

Manually Starting CSA

If you installed CSA with the Cisco IPICS server software, CSA starts automatically when the Cisco IPICS server boots up. If you stop CSA or if CSA stops on its own for any reason, you can restart CSA in the CSA utility or by entering CLI commands.

To start the CSA process from a terminal console session, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To start CSA, enter the following command:

```
[root]# service ciscosec start
```

Cisco IPICS displays the message [OK] after CSA starts.



CHAPTER 3

Troubleshooting the Cisco IPICS Server

This chapter describes how to resolve problems that you may encounter when you use the Cisco IPICS server and includes the following sections:

- [Troubleshooting Cisco IPICS Installation Issues, page 3-1](#)
- [Troubleshooting Cisco IPICS Administration Console Issues, page 3-2](#)
- [Troubleshooting User ID and Password Issues, page 3-24](#)
- [Troubleshooting License Issues, page 3-27](#)
- [Troubleshooting Policy Engine Issues, page 3-34](#)

Troubleshooting Cisco IPICS Installation Issues

For information about troubleshooting problems that you may experience when you install Cisco IPICS, refer to the “Troubleshooting the Installation” chapter in the [Cisco IPICS Server Installation and Upgrade Guide, Release 2.1\(1\)](#).

Troubleshooting Cisco IPICS Administration Console Issues

This section describes the issues that you may encounter with the Cisco IPICS Administration Console. These problems range from login issues to issues with viewing the information in the Administration Console.

This section includes the following topics:

- [Resolving Intermittent Browser Problems, page 3-3](#)
- [Resolving Failures to Access the Server With an Administration Console Browser Session, page 3-4](#)
- [Enlarging the Text in the Administration Console, page 3-9](#)
- [Reducing Text in the Administration Console, page 3-9](#)
- [Analyzing 404 or 500 Error Messages When You Attempt to Access the Administration Console, page 3-10](#)
- [Troubleshooting Browser Timeout Issues When You Configure an RMS with Twelve or More Loopback Interfaces, page 3-12](#)
- [Performing Database Procedures To Resolve Login Problems and Failure To Complete Tasks in the Administration Console, page 3-14](#)
- [VTG Activates Without Dispatcher Action, page 3-15](#)
- [Troubleshooting VTG Activation Problems, page 3-16](#)
- [VTG Does Not Appear on User PMC, page 3-17](#)
- [Troubleshooting an Ops View Save Failure, page 3-17](#)
- [Resolving Administration Console Undefined Errors, page 3-19](#)
- [Commands Fail Intermittently, page 3-20](#)
- [Adding Fonts to Internet Explorer to Fix Language Character Display Problems, page 3-20](#)
- [PMC Users Receive Error Messages During Login After a Database Restore Operation, page 3-21](#)
- [Configuration Changes Do Not Get Saved When Multiple Users Configure Cisco IPICS, page 3-22](#)
- [Recovering a Deleted System Administrator User, page 3-23](#)

Resolving Intermittent Browser Problems

Problem Your browser window does not reflect the latest configuration changes, or you experience intermittent problems with the Administration Console.

Solution Cisco IPICS supports only the use of Internet Explorer version 6.0.2. Be aware of the following browser-related guidelines and caveats when you use Cisco IPICS:

- By default, the Administration Console times out after 30 minutes of non use. When a timeout occurs, the system prompts you to log back in.



Note You may configure this session timeout period for a different duration by accessing the **Administration > Options** window and entering a new value in the Cisco IPICS Session Timeout Period field.

- As a best practice, make sure that you update your browser window often and before you perform any server administration tasks to ensure that you are working with the most current information. If you attempt to perform administration updates in a window that does not display the most current data, the update will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.
- To ensure that a current browser window displays the most current information, refresh it by clicking the button or tab that you used to display it. Cisco IPICS does not support the use of the browser Refresh button to refresh a window in the Administration Console.
- The Cisco IPICS Administration Console uses browser pop-up windows for certain functionality. If you have any browser pop-up blocker software installed on your machine, you may be prevented from performing certain actions. To ensure that you are not blocked from performing administration tasks, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.
- Cisco IPICS does not support accessing the Administration Console in more than one browser session at the same time on the same machine. If you use multiple browser sessions to access the Administration Console, you may

experience unexpected results. To ensure proper server operational behavior, do not open more than one browser session at a time on the same machine for Administration Console functions.

- To avoid browser-related memory issues, exit your browser and then restart it after prolonged use of the Cisco IPICS Administration Console.

Resolving Failures to Access the Server With an Administration Console Browser Session

Problem After you install Cisco IPICS, you cannot successfully connect to the Cisco IPICS server by using a browser session.

Solution You may encounter this problem if one of the following issues has occurred:

- You entered the incorrect IP address or DNS name for the Cisco IPICS server
- The tomcat service is not running
- The database server is not running
- A security setting on your computer has caused a required JavaScript add-on to become disabled

To resolve this problem, perform the following procedure:

Procedure

-
- Step 1** Check for the following items to make sure that the URL that you entered is correct:
- Ensure that you are using the secure HTTP URL, **https://** in the URL.
 - If you entered the IP address for the server, check that you entered the correct IP address in the Address field in your browser.
 - If you entered the DNS name for the server, ensure that the DNS name is correct and that your network is able to resolve the DNS name. If your network is unable to resolve the DNS name, enter the IP address in your browser.

Step 1 If you still cannot access the Administration Console, connect to the Cisco IPICS server via a terminal console by using the root user ID.

Step 2 Enter **root** in the *hostname login:* field and press **Enter**.

Cisco IPICS prompts you for the password for the root user ID.

Step 3 Enter the password for the root user ID and press **Enter**.

Step 4 Ensure that the tomcat service is running by entering the following command:

```
[root]# service ipics_tomcat status
```

Step 5 Perform one of the following actions, depending on the output that you receive:

- If the tomcat service is running, you receive output that is similar to the following example:

```
[root]# service ipics_tomcat status
Tomcat process (pid: 24025) is running on the system
```

If you receive output that indicates that the tomcat service is running, continue to [Step 11](#).

- If the tomcat service is not running, you receive output that is similar to the following example:

```
[root]# service ipics_tomcat status
PID_SEARCH_RESULT=
Tomcat is not running on the system.
```

If you receive output that indicates that the tomcat service is not running, continue with [Step 6](#).

Step 6 Restart the tomcat service and the policy engine by entering the following command:

```
[root]# service ipics restart
```



Note Be aware that Cisco IPICS cancels any active dial-in or dial-out calls when you enter the **service ipics restart** command.

Step 7 If the tomcat service does not restart, perform the following actions:

- a. Check whether Cisco IPICS already installed the crontab file by entering the following command:

```
[root]# crontab -l -u ipicsadmin
```

**Note**

The crontab file runs a process that checks if the tomcat service and database are running, and starts them if they are not running.

- b. If you receive a message that is similar to the following message, the tomcat cron file already exists. Continue to [Step 11](#).

```
[root]# crontab -l -u ipicsadmin
#-----
#
#  Module: ipicsadmin.cron - Cisco IPICS cron file for user
#  'ipicsadmin'
#
#  Usage: crontab < ipicsadmin.cron
#
#  Environment Variables:
#
#-----
SHELL=/bin/sh
MAILTO=root
HOME=/opt/cisco/ipics/tomcat

* * * * * /opt/cisco/ipics/bin/check_tomcat >>
/opt/cisco/ipics/tomcat/current/logs/ipicsadmin_cron.log 2>&1
```

- c. If you receive a message such as **no crontab for ipicsadmin**, continue with [Step 8](#).

Step 8 Install the crontab file by entering the following command:

```
[root]# crontab /opt/cisco/ipics/cron/ipicsadmin.cron
```

Cisco IPICS installs the crontab file.

Next, Cisco IPICS starts the tomcat service. You can then log in to the Administration Console by using your browser.

For information about checking the status of the tomcat service, see the [“Performing Tomcat Service Procedures” section on page 2-2](#).

Step 9 To check the status of the database, enter the following command:

```
[root]# onstat -
```

If the database is online and running, the command returns output that is similar to the following example.

```
IBM Informix Dynamic Server Version 10.00.UC1      -- On-Line -- Up
00:16:14 -- 124036 Kbytes
```

If the database is not running, the command returns output that is similar to the following example.

```
shared memory not initialized for INFORMIXSERVER 'IPICSDbServer'
```

If the command output indicates that the database is not running, continue to [Step 10](#).

- Step 10** If the database is not running, manually start the database server by entering the following command:

```
[root]# service ipics_db start
```

- Step 11** To verify network connectivity, enter the following command:

```
ping <default gateway IP address>
```

where:

<default gateway IP address> represents the default gateway address for your network.

- Step 12** If the ping command is not successful, unplug the network cable from interface 1 of the server, and connect it to interface 2.



Note

Generally, for servers that label their Ethernet interfaces as NIC 1 and NIC 2, you connect the Ethernet cable to the NIC 1 interface; this interface is usually the eth0 interface. For servers that label their Ethernet interfaces as 1 and 2, it is possible that the eth0 interface is mapped to interface 2. Consult your server product documentation to confirm the interface mapping.

- Step 13** Retry [Step 11](#) to attempt to verify server network connectivity.

- Step 14** If the ping command is successful, log in to another server on the network and attempt to ping the Cisco IPICS server.

If the ping command is not successful, troubleshoot the network connectivity with your network administrator.

- Step 15** Check the security settings on the PC that you use to access the Administration Console.

**Note**

For enhanced security, Cisco recommends that you review and follow the recommendations that are included in the Windows XP Security Guide. To find this document, refer to the Microsoft support site at <http://support.microsoft.com/> and search for “Windows XP Security Guide.”

When you follow the recommendations that are included in the Windows XP Security Guide and deny all add-ons, except those that are specifically allowed in the add-on list, you may encounter a problem where you cannot access the Administration Console. This issue occurs when you use Internet Explorer from a PC that runs Microsoft Windows XP SP2 and have not enabled the JavaScript GUID in the add-on list.

- Step 16** Change your security settings to ensure proper operation from Internet Explorer by explicitly enabling the following JavaScript GUID add-on on your PC:

GUID: {F414C260-6AC0-11CF-B6D1-00AA00BBBB58} - JavaScript

For detailed information about how to enable this add-on, refer to the Microsoft support site at <http://support.microsoft.com/> and search for Article ID 555235.

- Step 17** Try to access the server again by entering the IP address or DNS name, as shown below:

https://<ipaddress> | <dnsname>

where:

<ipaddress> or <dnsname> represents the IP address or DNS name of the server.

If you still cannot access the server, contact your Cisco technical support representative for assistance.

Enlarging the Text in the Administration Console

Problem You log in to the Administration Console successfully, but the text in the Administration Console is too small to be easily viewed.

Solution Your browser is configured to display text in a font that is smaller than the normal font. To enlarge the text in the Administration Console, perform the following procedure:

Procedure

- Step 1** Open a supported version of the Internet Explorer browser.
 - Step 2** From the menu bar of the browser, select **View > Text Size**.
 - Step 3** Select **Medium** or **Larger** from the list of options to enlarge the text size.
The text in the browser window displays in a larger font.
-

Reducing Text in the Administration Console

Problem You log in to the Administration Console successfully, but the text in the Administration Console is too large to be easily viewed.

Solution Your browser is configured to display text in a font that is larger than the normal font. To reduce the text in the Administration Console, perform the following procedure:

Procedure

- Step 1** Open a supported version of the Internet Explorer browser.
 - Step 2** From the menu bar of the browser, select **View > Text Size**.
 - Step 3** Select **Medium** or **Smaller** from the list of options to make the text size smaller.
The text in the browser window displays in a smaller font.
-

Analyzing 404 or 500 Error Messages When You Attempt to Access the Administration Console

Problem When you try to access the Cisco IPICS Administration Console after you perform a server software upgrade, the browser displays a 404 and/or 500 error message, as shown in the example below:

```
HTTP Status 404:
type Status report
message /ipics_server/
description: The requested resource (/ipics_server/) is not available.
```

```
Error: 500
Location: /ipics_server/
Internal Servlet Error:
```

Solution You may encounter these errors after you upgrade the server software and the system has cached some components that Cisco IPICS used in a previous version. Cached components may interfere with the proper operation of a newer version of the software and result in issues with the web application becoming unavailable and/or the occurrence of a general servlet (500) error, which causes the application to terminate unexpectedly after startup.

When this problem occurs, the system may display a message in the ipics.log file, as shown in the following example:

```
09:10:32,818 ERROR [/ipics_server]:3673 - Exception sending context
initialized event to listener instance of class
com.domain.ipics.server.core.ServerImpl
java.lang.ClassFormatError: Incompatible magic value 16693950 in class
file
```

Without access to the Administration Console **Serviceability > System Logs** window to view these log entries, you must manually access the log files by using CLI commands.

Perform the following procedure to manually access the log entries to look for the applicable error messages:

Procedure

- Step 1** Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software).
- Step 2** Log in to the server with root user privileges.
- Step 3** Change the directory by entering the following command:
- ```
[root]# cd tomcat/current/logs
```
- Step 4** Read the last 25 lines of the ipics.log file by entering the following command:
- Step 5** [root]# **tail -25 ipics.log**
- Step 6** Search the log for errors that indicate a problem with the web applications. These messages might contain the domain name (yourdomain.com). Messages relating to a 404 or 500 error also include phrases such as “Incompatible magic value” or “Class not found.”
- Step 7** If you determine that the Cisco IPICS web applications have become corrupted, delete one or more copies of the ipics\_server folder in the webapps location by entering the following command:

```
[root]# rm -rf /opt/cisco/ipics/tomcat/current/webapps/ipics_server
```



**Note** Be careful when you use the **rm** command with the **-rf** argument, because this command deletes files and folders without warning.

- Step 8** Delete the ipics\_server folder in the work location by entering the following command:
- ```
[root]# rm -rf /opt/cisco/ipics/tomcat/current/work/Catalina/localhost/ipics_server
```
- Step 9** Restart the tomcat service by entering the following command:
- ```
[root]# service ipics_tomcat restart
```
- The system displays a message to indicate whether the service has been restarted. When the tomcat service restarts, the system creates new ipics\_server folders.
- Step 10** Open a supported version of the Internet Explorer browser.
- Step 11** In the Location or Address field, enter the URL in the following format:
- ```
https://<ipaddress> | <dnsname>
```

where:

`<ipaddress>` is the IP address of the server and `<dnsname>` is the host name that you configured for the server.

You should be able to access the Administration Console.

Troubleshooting Browser Timeout Issues When You Configure an RMS with Twelve or More Loopback Interfaces

Problem When using a high latency, low bandwidth connection, you may encounter browser timeout errors when you try to update the RMS configuration for any RMS that is configured with twelve or more loopback interfaces.

Solution To resolve this issue, you must modify the Internet Explorer settings on your PC to adjust the timeout duration. This configuration modifies the ReceiveTimeout data value to allow for the additional delay.



Caution

Please use extreme caution when you modify the registry. If you are not familiar with editing the registry, you should seek technical support assistance before you perform this procedure. If you modify the registry incorrectly, you may need to reinstall the operating system. Therefore, make sure that you back up the registry before you modify it and are aware of how to restore the registry, if a problem occurs.



Tip

For more information about how to back up, restore, and modify the registry, access the Microsoft Support site at <http://support.microsoft.com> and search the Microsoft Knowledge Base for a description of the Microsoft Windows registry.

To modify the ReceiveTimeout data value, perform the following procedure on the PC that you use to access the Cisco IPICS Administration Console:

Procedure

- Step 1** On the PC that you use to access the Administration Console, choose **Start > Run**.
- Step 2** In the Open dialog box, enter **regedit**.
The Registry Editor displays.
- Step 3** Click the + sign that displays next to the **HKEY_CURRENT_USER** entry.
The folders that contain root configuration information for the user who is currently logged in display.
- Step 4** Click the + signs that display next to each of the folder names to navigate to the **Software\Microsoft\Windows\CurrentVersion** folder.
- Step 5** Click the + sign that displays next to the **Internet Settings** folder.
At this point, you have navigated to the following folder:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings.
- Step 6** In the Internet Settings folder, look for the **ReceiveTimeout** name.
- Step 7** To modify this setting, right-click the **ReceiveTimeout** name; then, click **Modify**.
The Edit DWORD Value dialog box displays. The current DWORD value displays in hexadecimal format.

Alternatively, you can choose to delete the ReceiveTimeout name altogether by clicking **Delete**. If you choose to take this action, be aware that you could wait indefinitely for the server to respond.
- Step 8** Click the **Decimal** radio button to display this value in decimal format.
- Step 9** To configure this value to the recommended setting to accommodate high latency, low bandwidth links, enter **480000** in the Value data field.
This modification configures the timeout value to 8 minutes.
- Step 10** Click **OK** to save your change.
- Step 11** To exit the Registry Editor, choose **Registry > Exit**.
- Step 12** Restart your PC for the change to become effective.
-

Performing Database Procedures To Resolve Login Problems and Failure To Complete Tasks in the Administration Console

Problem Users who are currently logged in to the system encounter errors when they try to perform tasks and new users cannot log in to the Administration Console. Existing VTGs and channel connections function normally.

Solution You may encounter this problem under the following conditions:

- The database has stopped.
- The database has entered into quiescent mode. This mode occurs when a restore operation or database maintenance is being performed.

If the database has stopped or gone into quiescent mode, you can perform procedures to restart the database.

To troubleshoot this issue, perform the following procedure:

Procedure

-
- Step 1** Check to make sure that the database is running by following these steps:
- a. Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software).
 - b. Log in to the server with the root user ID.
 - c. Check to see if the database is running by entering the following command:
[root]# **onstat -**
 - If the database is online and running, the command returns the following response; continue to [Step 5](#).


```
IBM Informix Dynamic Server Version 10.00.UC1      -- On-Line --
Up 00:16:14 -- 124036 Kbytes
```
 - If the database is in quiescent mode, the command returns the following response; continue to [Step d](#).


```
IBM Informix Dynamic Server Version 10.00.UC1      -- Quiescent
-- Up 00:00:42 -- 124036 Kbytes
```
 - If the database is not running, the command returns the following response; continue to [Step 2](#).

```
shared memory not initialized for INFORMIXSERVER
'IPICSDBServer'
```

- d. If the database is in quiescent mode and a restore operation is in progress, wait for the operation to complete.
- e. If you are not currently restoring the database, move the database from maintenance mode to online mode by entering the following command:

```
[root]# onmode -m
```

Step 2 If the database is stopped, you can start it by entering the following command:

```
[root]# service ipics_db start
```

If the database successfully starts, the Cisco IPICS operating system displays the message [OK].

Step 3 If the database does not successfully start, check the diagnostics.log file by entering the following command:

```
[root]# more /opt/cisco/ipics/database/logs/diagnostics.log
```

Step 4 Press the **Spacebar** to view all the messages in the log file. To close the message log file, press **q**.

If you cannot resolve the problem by using the information that appears in the diagnostics.log file, contact your Cisco support personnel.

Step 5 If the database is running properly and you cannot use the Administration Console, contact your Cisco technical support representative for assistance.

VTG Activates Without Dispatcher Action

Problem From the **VTG Management > VTG Workgroups** window in the Administration Console, you see that a VTG is active, even though you did not activate it.

Solution You may encounter this situation if one of the following instances have occurred:

- The VTG was triggered by a policy. To check if Cisco IPICS recently activated any policies that contained the VTG, navigate to the **Policy Management > Execution Status > Executing/Executed Policy** tab.

- Another dispatcher is logged in to your Cisco IPICS system and activated that VTG.

**Note**

As a best practice, make sure that you refresh your browser window often and before you perform any server administrative functions to ensure that you are working with the most current information. If you attempt to perform an administrative refresh in a window that does not display the most current data, the refresh will not succeed and Cisco IPICS will display an error. If this situation occurs, refresh your browser window and retry the operation.

Troubleshooting VTG Activation Problems

Problem You activate a policy, but one of the VTGs in the policy does not activate.

Solution The system may have insufficient resources, such as unavailable multicast addresses, to activate the entire policy. In such cases, Cisco IPICS attempts to activate as much of the policy as it can (for example, activating two of the three VTGs in a policy, if the system has only two available multicast addresses). To attempt to fix the problem, perform the following procedure:

Procedure

-
- Step 1** Navigate to the **Policy Management > Execution Status > Executing/Executed Policy** tab.
 - Step 2** Locate the policy that you activated.
 - Step 3** Click **+** next to the policy name to expand it.
 - Step 4** Check the Status field in any rows that contain **ActivateVTG** in the Action Type field.
 - Step 5** If the status displays as Failed, click **Details** in the Message field.
The Message popup window displays with detailed information about the activation failure.

Step 6 If you can determine the cause of the problem from the information in the Message window, perform appropriate actions to fix the problem.

For example, the following message might indicate that the problem may be due to an insufficient number of available multicast addresses:

```
Activate VTG:vtgname has FAILED.Failed to activate talkgroup
```

VTG Does Not Appear on User PMC

Problem The dispatcher adds a user to a VTG, but the user does not see the VTG appear on the PMC. The user may also not see channels that the operator associates to the user profile.

Solution This problem occurs when a user is logged in to the database under two different user IDs. The user may log in with one user ID, while the operator or dispatcher uses another ID for the user.

Check the **User Management > Users** window for users that have multiple user IDs and delete the extra IDs.

Troubleshooting an Ops View Save Failure

Problem When you try to save an ops view that you added, the following error message displays:

```
Cisco IPICS could not save ops view <opsview name>
```

where:

<opsview name> is the name of the ops view that was being saved.

Solution Cisco IPICS may display this error message because of various situations, such as a database problem or an issue with another system component. If you encounter this error, take the following action:

Procedure

-
- Step 1** Log in to the Cisco IPICS Administration Console by using the ipics user ID.
- Step 2** Navigate to the **Serviceability > System Logs** window.
- Step 3** Review the logs in the **Recent System Log Entries** pane. Check for any errors that display in red or blue text and which appear to be related to ops views.
- Step 4** If you cannot find any errors that are related to ops views in the Recent System Log Entries pane, click **Download** to download the activity logs to your computer.
- Step 5** Unzip the **ipics.zip** file and save the ipics.log file to your computer.
- Step 6** Open the **ipics.log** file as a text file.



Note To view the log file, you must use a text file viewer that can understand UNIX newline characters, such as Wordpad. If you use Notepad, the file will not display properly.

- Step 7** Search for the word “ERROR” in the ipics.log file.
- The ipics.log may help you to determine the cause of the failure so that you can resolve the problem.
- If you are not able to determine the specific error that has occurred or find information in the ipics.log file that may help you to isolate the problem, proceed to [Step 8](#).
- Step 8** Check to determine if the database is running by logging in to the Cisco IPICS server by using the root user ID and entering the following command:
- ```
[root]# onstat -
```
- Step 9** Perform one of the following actions, depending on the output that displays:
- If the database is not running, the command displays text that is similar to the following example.
 

```
shared memory not initialized for INFORMIXSERVER 'IPICSDbServer'
```

If you determine that the database is not running, proceed to [Step 10](#).
  - If the database is online and running, the command displays text that is similar to the following example.

```
IBM Informix Dynamic Server Version 10.00.UC1 -- On-Line -- Up
00:16:14 -- 124036 Kbytes
```

If you determine that the database is running, contact your Cisco technical support representative for assistance.

**Step 10** If the database has stopped, you can start it by entering the following command:

```
[root]# service ipics_db start
```

If the database successfully starts, the system displays the message [OK].

If the database does not successfully start, check the diagnostics.log file by entering the following command:

```
[root]# more /opt/cisco/ipics/database/logs/diagnostics.log
```

**Step 11** Press the **Spacebar** to view all the messages in the log file. To close the message log file, press **q**.

If you cannot resolve the problem by using the information that appears in the diagnostics.log file, contact your Cisco support personnel.

---

## Resolving Administration Console Undefined Errors

**Problem** Administration Console users cannot view any windows that display data in a table format, and receive errors that indicate that elements in the Administration Console are undefined.

**Solution** This problem occurs when the browser JavaScript engine cannot process advanced dynamic features because of installation of third party software or other setup issues. You can resolve this problem by reinstalling the JavaScript engine. To download the installation script to your PC, go to <http://www.microsoft.com> and search for Windows Script 5.6 for Windows Server 2003.

## Commands Fail Intermittently

**Problem** An intermittent “command failed” error displays when a dispatcher activates or deactivates a VTG or when a user logs in or logs out of the PMC application.

**Solution** Retry the command or action. For more information about the nature of the error, navigate to the **Serviceability > System Logs** window in the Administration Console and view the logs in the **Recent System Log Entries** window. The log content should provide you with additional details about the command failure.

## Adding Fonts to Internet Explorer to Fix Language Character Display Problems

**Problem** Some data, such as user names and channel names, displays with incorrect characters in some languages.

**Solution** The Internet Explorer browser on some PCs may be unable to display characters from several languages on the same page. When the browser displays English, Hebrew, and Arabic, characters from some of the languages may display incorrectly. The problem occurs when Internet Explorer selects a font that supports only some languages.

To resolve this problem, in Internet Explorer, choose a font that supports all unicode character sets. Such fonts include Arial Unicode MS (which is included with Microsoft Office).

To choose a new font for Internet Explorer, perform the following procedure:

### Procedure

---

- Step 1** Open a supported version of the Internet Explorer browser.
- Step 2** From the Internet Explorer menu, choose **Tools > Internet Options**.  
The Internet Options window displays.
- Step 3** Click **Fonts**.  
The Fonts dialog box displays.

- Step 4** From the Web page font pane, select Arial Unicode MS.
- Step 5** To accept the font choice, click **OK**.
- Step 6** Click **OK** to save your changes and close the Internet Options window. Internet Explorer now displays the languages correctly.
- 

## PMC Users Receive Error Messages During Login After a Database Restore Operation

**Problem** After a database restore procedure completes, PMC users receive an “unknown response” error message when they try to launch the PMC. These users cannot connect to the server but they can operate in offline mode.

**Solution** This problem may occur if the tomcat service does not restart after the restore procedure has completed or if the PMC user attempts to log in to the system before the tomcat service has completed the restart process.

To resolve this problem, perform the following procedure:

### Procedure

---

- Step 1** Check to determine if the tomcat service is running by entering the following command:
- ```
[root]# service ipics_tomcat status
```
- Step 2** Perform one of the following actions, depending on the output that you receive:
- If the tomcat service is running, you receive output that is similar to the following example:

```
[root]# service ipics_tomcat status  
Tomcat process (pid: 24025) is running on the system
```

If you receive output that indicates that the tomcat service is running, wait for at least five minutes so that the database has time to synchronize its information with the RMS.
 - If the tomcat service is not running, you receive output that is similar to the following example:

```
[root]# service ipics_tomcat status
PID_SEARCH_RESULT=
Tomcat is not running on the system.
```

If you receive output that indicates that the tomcat service is not running, restart the tomcat service and the policy engine by entering the following command:

```
[root]# service ipics restart
```

**Note**

Cisco IPICS cancels any active dial-in or dial-out calls when you enter the **service ipics restart** command.

Step 3 If you continue to experience problems, contact your Cisco technical support representative for assistance.

Configuration Changes Do Not Get Saved When Multiple Users Configure Cisco IPICS

Problem Multiple users are connected to the Administration Console with separate browser sessions and are making configuration changes concurrently. One user changes a configuration. At a later time, the user notices that their changes were overwritten or not saved.

Solution If multiple users configure Cisco IPICS at the same time, and the users are updating the same data, Cisco IPICS retains the last change that was made. The last configuration change prevails over any other previous configuration changes to the Cisco IPICS Administration Console.

Recovering a Deleted System Administrator User

Problem You deleted the last user who had the System Administrator or All role, and now you cannot perform any system administration tasks in the Administration Console.

Solution If you delete all system administrator users from the system, you can log in as an operator and create a new system administrator user ID. Cisco IPICS includes a safeguard that prevents you from deleting all operators from the system.

**Note**

You must be assigned the operator role and have an operator user ID and password to recover a deleted system administrator user. For more information about operators, refer to the “Performing Cisco IPICS Operator Tasks” chapter in the [*Cisco IPICS Server Administration Guide, Release 2.1\(1\)*](#).

To recover the system administrator role, perform the following procedure:

Procedure

- Step 1** Log in to the server by using the operator user ID and password.
- Step 2** From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.
- Step 3** Click **Add**.
- Step 4** In the required fields, which are indicated by an asterisk, enter the user information.
- Step 5** From the Roles drop-down list box, choose **System Administrator** or **All** for the user role.

The new user appears in the SYSTEM ops view; this user can now perform administrative tasks.

Troubleshooting User ID and Password Issues

The following section describes how to troubleshoot issues that you may encounter with user IDs and passwords.

This section includes the following topics:

- [Resetting a Forgotten or Missing ipics User Password, page 3-24](#)
- [Resetting the Password for the ipicsadmin or informix User ID, page 3-24](#)
- [Changing the root User Password, page 3-25](#)
- [Resetting a Locked or Disabled User Account, page 3-26](#)

Resetting a Forgotten or Missing ipics User Password

Problem You attempt to log in to the Administration Console as the ipics user. A pop-up window displays to inform you that you have entered an incorrect user ID or password.

Solution You entered an incorrect password for the ipics user. If you have root user access, you can reset the ipics user password and regain access to the Administration Console by entering the **reset_pw** command.

To reset the ipics user ID and resolve this problem, perform the procedure that is documented in the [“Resetting, Changing, or Creating a Password With the reset_pw Tool”](#) section on page 6-7.

Resetting the Password for the ipicsadmin or informix User ID

Problem You attempt to log in to a terminal console as the ipicsadmin or informix user to perform database administration tasks. You cannot retrieve the password for the informix user, or you have lost or forgotten the password for the ipicsadmin user. You are not able to log in to the system.

**Note**

You create a password for the ipicsadmin user during the installation of the Cisco IPICS server software. The installation program also creates a password for the informix user by using a random algorithm; however, you cannot retrieve this password.

Solution If you have root user access, you can log in by using the ipicsadmin or informix user ID by entering either the **su** command or by entering the **reset_pw** command to reset the ipicsadmin or informix password.

To log in as the informix or ipicsadmin user, perform the following procedure:

Procedure

- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** Log in as the ipicsadmin or informix user by performing one of the following actions:
- To log in as the ipicsadmin user, enter the following command:
[root]# **su - ipicsadmin**
 - To log in as the informix user, enter the following command:
[root]# **su - informix**
- Step 3** After you have completed your tasks as the ipicsadmin or informix user, enter **exit** to log out as that user and return as the root user.
-

To reset the password for the ipicsadmin or informix user, perform the procedure that is documented in the [“Resetting, Changing, or Creating a Password With the reset_pw Tool”](#) section on page 6-7.

Changing the root User Password

Problem You need to change the root user password.

Solution You can change the password for the root user ID, as needed, by performing the procedure that is documented in the [“Resetting, Changing, or Creating a Password With the reset_pw Tool”](#) section on page 6-7.

Resetting a Locked or Disabled User Account

Problem A user whose account has been locked or disabled cannot log in to the system.

Solution The user account may be locked or disabled. A user account can be locked or disabled under the following conditions:

- The number of invalid login attempts exceeded the number of maximum attempts and Cisco IPICS automatically locked the user. For more information, refer to the “Performing Cisco IPICS System Administrator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- A user with Operator or All privileges manually locked or disabled the user. For more information about locking out or disabling a user, refer to the “Performing Cisco IPICS Operator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

When a user account is disabled, Cisco IPICS disallows any endpoint devices from logging in to the system; any existing login sessions, such as PMC, dial-in, and Administration Console, are automatically terminated.

When a user account is locked, Cisco IPICS disallows any new logins; existing logins continue to work until the user logs out of the system.

To unlock or enable a user account, perform one of the following actions:

- If you have access to the root user ID, perform the procedure that is documented in “Unlocking or Enabling a Locked or Disabled User With the *enableuser Tool*” section on page 6-3 to unlock or enable the user with CLI commands.
- If you are able to access the Administration Console with a user ID that has Operator or All privileges, perform one of the following actions to unlock or enable a user account; then, proceed to verify your configuration changes:
 - To unlock a user account in the Administration Console, follow the procedure in the “Locking or Unlocking a User” section in the “Performing Cisco IPICS Operator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

- To enable a user account in the Administration Console, follow the procedure in the “Changing User Status” section in the “Performing Cisco IPICS Operator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Troubleshooting License Issues

This section contains information about troubleshooting problems with your Cisco IPICS license and includes the following topics:

- [Resolving Invalid Base Server License Messages that Display After You Upload the License File, page 3-27](#)
- [After Uploading Multiple License Files, All Features Do Not Display in the Administration Console, page 3-31](#)
- [After Changing the Server IP Address, You Experience Host Name Mismatch or Problems Installing the License, page 3-32](#)
- [Changing System Date Invalidates Time-Bound License, page 3-32](#)
- [Suppressing Server Expiration Messages After Installing a More Recent Time-Bound License, page 3-33](#)

Resolving Invalid Base Server License Messages that Display After You Upload the License File

Problem You upload the license for your Cisco IPICS server in the **Administration > License Management** window. After you click **Apply** to apply the license, the following message persists in the Administration Console:

Your system does not have a valid base server license; please upload this license file type.

You cannot navigate to any other windows in the Administration Console.

Solution This situation might be caused by one or more of the following conditions:

- The license file is invalid

- The license manager does not recognize the license file as a valid file and does not run
- The license manager did not start
- Unnecessary files in the directory in which Cisco IPICS stores the licenses are causing problems with the license manager

**Note**

You can encounter license issues if you change the IP address of the server using an unsupported method. To change the server IP address, use the **modify_ip** command by following the procedure that is documented in the [“Changing the Server IP Address With the modify_ip Tool” section on page 6-4](#). Using other methods to change the server IP address can cause host mismatch problems and invalidate the license.

To resolve these conditions, perform the following procedure:

Procedure

-
- Step 1** To determine that you have a valid license, check the following items:
- Make sure that the MAC address for the license file matches the MAC address of the eth0 interface of the Cisco IPICS server. To locate the hardware MAC address for the eth0 interface, log in to the server by using the root user ID; then, enter the following command and note the information that displays in the HWaddr field in the command output:

```
[root]# ifconfig eth0
```
 - Make sure that the license file has a file extension of .lic.
 - Make sure that there are no spaces or special characters in the name of the license file.
- Step 2** If you determine that your license file is invalid or misnamed, purchase a valid license file or obtain a new copy of your existing file. For more information, refer to the “Obtaining Your License File” section in the “Installing Cisco IPICS” chapter in the [Cisco IPICS Server Installation and Upgrade Guide, Release 2.1\(1\)](#).
- Step 3** From the Administration Console, navigate to the **Administration > License Management** window; then, click the **Apply** button to restart the license manager.

Step 4 If the server continues to display the invalid license message, log in to the server by using the root user ID.

Step 5 To check the status of the license file, enter the following command:

```
[root]# service ipics_lm status
```

Step 6 Perform the following action, depending on the message that Cisco IPICS displays:

- If the following message displays, the license manager is not running. Continue with [Step 7](#).

```
ipics_lm is not running.
```

- If the following message displays, the license manager is running. Proceed to [Step 10](#).

```
ipics_lm is running (PID 24856).
```

**Note**

The license manager does not start until it detects a valid license file. If the license manager does not reflect a running status after you upload a license file, this condition could indicate that the license manager does not recognize a valid license file.

Step 7 If the license manager is not running, restart the license manager by entering the following command:

```
[root]# service ipics_lm restart
```

Step 8 To recheck the status of the license manager, enter the following command:

```
[root]# service ipics_lm status
```

Step 9 Perform one of the following actions, depending on the message that displays:

- If a message displays to indicate that the license manager is running, proceed to [Step 10](#).
- If a message displays to indicate that the license manager is not running, continue with [Step 11](#).

Step 10 To check for unnecessary files, delete them, and upload license files, perform the following steps:

- a. Log in to the Cisco IPICS server by using the root user ID.

- b. To navigate to the directory that includes the license files, enter the following command:

```
[root]# cd /root/tomcat/current/webapps/license
```
- c. Remove all of the license files that are in the `/root/tomcat/current/webapps/license` directory by entering the following command:

```
[root]# rm *.lic
```
- d. Enter **yes** when the system prompts you to confirm the deletion of each license file.



Note Make sure that you do not remove any other files in this directory. The `cisco.opt` file in this directory is required for the correct operation of Cisco IPICS.

- e. Upload the license file(s) by following the procedure in the “Uploading the Cisco IPICS License Files” section in the “Installing Cisco IPICS” chapter in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.



Note Be sure to click **Apply** after you upload each file.

Step 11 If you still cannot upload the license file, perform the following steps:

- a. To create a log file and a .tar file that contain diagnostic and logging information, enter the following command:

```
[root]# /opt/cisco/ipics/bin/diagnosticscript <output-file-name>.log  
<tar-file-name>.tar
```

where:

`<output-file-name>.log` is the name that you designate for the log file, and
`<tar-file-name>.tar` is the name that you designate for the .tar file.

- b. Save, to your PC, the .tar file that you created in Step a. by following the procedure that is documented in the “Downloading the Server Diagnostic Information” section in the “Understanding Cisco IPICS Serviceability and Diagnostic Information” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

- c. If you require further assistance, contact your Cisco technical support representative; you may need to provide the .tar file.
-

After Uploading Multiple License Files, All Features Do Not Display in the Administration Console

Problem You uploaded multiple license files, but the summary in the **Administration > License Management** window does not display all of the features that you have licensed.

Solution Perform the following actions to make sure that the name of the license file matches the MAC address of the server eth0 interface so that the license manager can read each license correctly.

Procedure

- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** To navigate to the directory that includes the license files, enter the following command:

```
[root]# cd tomcat/current/webapps/license
```
- Step 3** Remove all of the license files that are in the **tomcat/current/webapps/license** directory by entering the following command:

```
[root]# rm *.lic
```
- Step 4** Enter **yes** when the system prompts you to confirm the deletion of each license file.



Note Do not remove any other files in this directory.

- Step 5** From the Administration Console, navigate to the **Administration > License Management** window.

- Step 6** Upload the license file(s) by following the procedure that is documented in the “Uploading the Cisco IPICS License Files” section in the “Installing Cisco IPICS” chapter in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.



Note Make sure that each license file has the correct MAC address.

After Changing the Server IP Address, You Experience Host Name Mismatch or Problems Installing the License

Problem After you reboot your server, following an IP address change, you cannot apply the license file. The following message persists in the Administration Console and you cannot navigate to any area in the Administration Console except the **Administration > License Management** window:

```
Your system does not have a valid base server license; please upload
this license file type.
```

Solution Some methods of changing the IP address do not update the `/etc/hosts` file, which can cause host mismatch or other IP connectivity problems. To ensure that Cisco IPICS properly processes any IP address changes, use only the **modify_ip** tool to change the IP address by following the procedure that is documented in the “[Changing the Server IP Address With the modify_ip Tool](#)” section on page 6-4.

Changing System Date Invalidates Time-Bound License

Problem After you change the server date, your time-bound license becomes invalid.

Solution Cisco IPICS can invalidate time-bound licenses when you change the system date in the operating system to a date that is before the license start date. Invalid licenses cause the Cisco IPICS system to become inoperable.



Note You must restart the license manager, or reboot the server, for system date changes to become effective.

To resolve issues that pertain to these system date changes, perform the following procedure:

Procedure

-
- Step 1** Open a terminal window and log in using the root user ID.
- Step 2** Change the system date to a date that is after the system start date by entering the following command:
- ```
[root]# date mmdyyy
```
- where:
- mmdyyy* is the current date.
- Step 3** Restart the license manager by entering the following command:
- ```
[root]# service ipics_lm restart
```
-

Suppressing Server Expiration Messages After Installing a More Recent Time-Bound License

Problem You have existing time-bound licenses, and you install a more recent time-bound license on your server. After the installation, you continue to see warning messages that alert you of an upcoming license expiration.

Solution You may see the license expiration warning message if you do not remove additional time-bound licenses from the server. To suppress this warning message, remove the time-bound licenses that are about to expire by performing the following procedure:

Procedure

-
- Step 1** Open a terminal window and log in by using the root user ID.

- Step 2** Navigate to the directory where Cisco IPICS stores the license files by entering the following command:
- ```
[root]# cd tomcat/current/webapps/license
```
- Step 3** View the license files by entering the following command:
- ```
[root]# ls -l *.lic
```
- The license files display with the time and date that the license was last modified.
- Step 4** Make a note of the licenses that you no longer need.
- The time and date that displays with the file information might assist you with determining which files you need to delete.
- Step 5** Delete the unnecessary license files by entering the following command:
- ```
[root]# rm <licensefilename>.lic
```
- where:
- <licensefilename>.lic* is the name of the license file that you want to delete.

**Caution**


---

Make sure that you do not delete the cisco.opt file. This file is required for the correct operation of Cisco IPICS.

---

- Step 6** Repeat [Step 5](#) for each license file that you need to delete.
- Step 7** Restart the server by entering the following command:
- Step 8** `[root]# service ipics restart`
- Step 9** Log in to the Administration Console by using the ipics user ID and navigate to the **Administration > License Management** window.
- Step 10** To apply the license deletions to the system configuration, click **Apply**.
- Step 11** If a message displays that indicates that a license is about to expire, click **Dismiss Warnings**.
- 

## Troubleshooting Policy Engine Issues

This section contains information about troubleshooting problems with the policy engine and includes the following topics:

- [Uploading a Large Zipped File of Prompts Causes an Error](#), page 3-35
- [IppeAgentImpl ERROR Messages Display in the ipics.log File](#), page 3-36
- [Resolving Communication Problems Between the Policy Engine and the Prompt Manager](#), page 3-38
- [Resolving Reconnection Failures After a Dial-In Caller Uses the Hold or Call Waiting Feature](#), page 3-38
- [Troubleshooting Dial-In Call Connection Failures](#), page 3-39
- [Troubleshooting Dial-Out Invitation Failures](#), page 3-43
- [Troubleshooting Dial-Out Notification Failures](#), page 3-44
- [Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views](#), page 3-46
- [Understanding a PARTIAL\\_SERVICE Status For the Dial Engine and Subsystem Manager](#), page 3-46
- [Analyzing a SHUTDOWN Status For the SIP Subsystem](#), page 3-47

## Uploading a Large Zipped File of Prompts Causes an Error

**Problem** From the Administration Console, you attempt to upload a large zipped file that contains dial engine prompts and see the following error message:

The form could not be properly constructed.

When you view the system logs from the **Serviceability > System Logs** window, the following error messages display:

```
java.lang.IllegalArgumentException: invalid directory: \\CHANNEL\
 at com.cisco.file.File.<init> (L885)
 at com.cisco.file.File.<init> (L724)
 at
com.cisco.ivr.config.api.impl.ManageRepositoryAPI.getFileList (L143)
 at com.cisco.ivr.config.api.impl.ManagePrompts.getFileList (L383)
 at com.cisco.ivr.config.api.impl.ManagePrompts.getPromptList (L369)
 at
com.cisco.ipics.ippe.dialengine.promptmanagement.handlers.PromptHandle
r.getPromptList (L215)
 at
com.cisco.ipics.ippe.dialengine.promptmanagement.actions.PromptAction.
doInit (L444)
```

```

 at
com.cisco.ipics.ippe.dialengine.promptmanagement.actions.PromptAction.
unspecified(L152)

```

**Solution** You attempted to upload a zipped file that is larger than Cisco IPICS can handle. Cisco IPICS can upload zipped files with a maximum size of 1024 MB (1 GB). To resolve this problem, create a smaller zipped file or divide the zipped file into smaller zipped files; then, retry the upload process.

## IppeAgentImpl ERROR Messages Display in the ipics.log File

**Problem** When you view the system logs that are located in the **Serviceability > System Logs** window in the Administration Console, you see an error message that is similar to the following example:

```

2007-02-06 21:19:45,000 [http-8443-Processor68] ERROR
IppeAgentImpl:200 -
com.cisco.ipics.ippe.communicator.subsystem.IppeSubsystemRemoteService

```

**Solution** Error messages that include IppeAgentImpl in the text indicate that your system could not connect to the Cisco IPICS policy engine. This message may display because your system is not licensed for the policy engine, or the policy engine processes did not start.



### Note

---

Messages that display INFO in the ipics.log file are only for informational purposes and do not signify a problem with the policy engine.

---

If your system is not licensed for the policy engine, no action is required. To determine if your system is licensed and to check the status of the policy engine, perform the following procedure.

### Procedure

- 
- Step 1** Check that your system is licensed for the policy engine by navigating to the **Administration > License Management > Summary** window in the Server tab of the Administration Console.
  - Step 2** Check the status of your license in the Policy Engine Base License field.

If the field shows a status of Not Licensed, IppeAgentImpl messages typically display in the logs and require no action.

If the field shows a status of Licensed, continue with [Step 3](#).

**Step 3** Perform the following steps to check if the policy engine processes are running and restart them, if necessary:

- a. Open a terminal window and log in to the server by using the root user ID.
- b. To check the status of the policy engine processes, enter the following command:

```
[root]# service ippe_dial_engine status
```

If the policy engine processes are running, Cisco IPICS displays information similar to the following text:

```
CVD process (pid 7606) is running...
Engine process (pid 7714) is running...
```

If the policy engine processes are not running, Cisco IPICS displays information similar to the following text:

```
CVD process is NOT running...
Engine process is NOT running...
```

- c. If the policy engine processes are not running, start them by entering the following command:

```
[root]# service ippe_dial_engine start
```

Cisco IPICS displays the message [OK] as each process starts.

- d. Check the status of the policy engine by reentering the **service ippe\_dial\_engine status** command.
  - e. If the policy engine processes are not running, contact your Cisco technical support representative for assistance.
-

## Resolving Communication Problems Between the Policy Engine and the Prompt Manager

**Problem** You encounter errors with the policy engine; messages that are similar to the ones shown below display in the **Serviceability > System Logs** window or in the ipics.log file:

```
2006-08-18 14:20:53,961 [http-8443-Processor25] ERROR PromptUtil:200 -
Unable to communicate with prompt manager.
2006-08-18 14:20:53,962 [http-8443-Processor25] ERROR PromptUtil:200 -
Unable to communicate with prompt manager.
2006-08-18 14:20:56,747 [http-8443-Processor21] ERROR PromptUtil:200 -
```

**Solution** This situation indicates that the policy engine processes are not running. To start the policy engine processes, perform the procedure that is documented in the [“Manually Starting the Dial Engine”](#) section on page 2-15.

## Resolving Reconnection Failures After a Dial-In Caller Uses the Hold or Call Waiting Feature

**Problem** After dialing in and connecting to a channel with a Cisco Unified IP Phone, you receive another call. You place the dial-in call on hold and use the call waiting feature to answer the incoming call. When you attempt to reconnect with the channel, you receive several seconds of silence, followed by a fast busy tone.

**Solution** The Cisco Unified IP Phone requires Media Termination Point (MTP) resources to use the hold or call waiting feature. MTP resources must exist in your SIP provider (for example, Cisco Unified Communications Manager) to successfully reconnect to a dial-in call after you use the hold or call waiting feature.

To successfully reconnect with a dial-in call, either add MTP resources to your SIP provider, or configure your SIP provider so that it can allocate MTP resources from another source. For more information about configuring the SIP provider, refer to the “Configuring the SIP Provider” sections of the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in the [Cisco IPICS Server Administration Guide, Release 2.1\(1\)](#).

# Troubleshooting Dial-In Call Connection Failures

**Problem** When you call in to the Cisco IPICS policy engine, your call does not connect. Instead, you hear a fast busy tone or a message that indicates that the call cannot be completed.

**Solution** One or more of the following conditions can cause dial-in calls to fail to connect:

- Your dial engine or ops view configuration might be incorrect
- The policy engine was not manually restarted after you performed SIP configuration changes
- The **bind control source-interface Loopback0** command was not successfully applied to your RMS configuration
- The dial peer configuration for the RMS might be incomplete or incorrect. Problems with dial-in and dial-out calls can be caused by incorrect or misconfigured dial peers. For information about configuring your dial peers for use with Cisco IPICS, refer to the “Configuring the Cisco IPICS RMS Component” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

To resolve this issue, perform the following procedure:

## Procedure

---

**Step 1** Check your ops view configuration to make sure that a dial number and dial ports are associated with an ops view by navigating to the **Configuration > Ops Views** window in the Server tab.

The Ops Views window displays.

**Step 2** Check to make sure that a dial-in number exists in the ops view configuration and enter a number if it does not exist by following these steps:

- a. Click the name of the ops view.  
The **Ops Views > <opsviewname>** window displays.
- b. Determine if a dial-in number exists in the ops view configuration by checking the Dial Number field in the General tab.
- c. If the Dial Number field is empty, enter the dial-in information in this field.

For information about adding a dial-in number for an ops view, refer to the “Performing Ops Views Tasks” section of the “Configuring and Managing Cisco IPICS Operational Views” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

**Step 3** Determine if dial port licenses have been allocated for the ops view by viewing the Dial Ports field in the License Allocation pane.

**Step 4** If the number in the Dial Ports field is 0, increase the number to allocate sufficient licenses for dial ports in the ops view.

For information about allocating dial ports for an ops view, refer to the “Allocating Dial Ports for the Dial-In/Invite and Notification Features” section of the “Configuring and Managing Cisco IPICS Operational Views” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

**Step 5** Check to make sure that a sufficient number of dial ports exist for dial-in calls in the ops view by viewing the following fields:

- Dial ports reserved for dial-in/invite feature
- Dial ports reserved for dial-in/invite or notifications

**Step 6** If the number that displays in the fields in [Step 5](#) is equal to zero, decrease the number of ports in the **Dial ports reserved for notifications** field; then, perform one of the following actions:

- Add the ports that you removed to the **Dial ports reserved for dial-in/invite feature** field.
- Take no action. Cisco IPICS adds the ports that you removed to the total number of ports that are reserved for the dial-in/invite feature and notifications.

**Step 7** Make sure that you have specified a host, user name, and password for the SIP provider by navigating to the **Dial Engine > SIP Configuration** window; then, view the fields that display in the SIP Provider Configuration pane.

**Step 8** If any fields in the SIP Configuration window are missing or incorrect, add or change them.

For more information about configuring SIP, refer to the “Configuring SIP” and “Configuring the SIP Provider” sections of the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

**Step 9** Perform the following steps to make sure that the proper SIP configuration has been applied to the RMS:



**Note**

If you enter the **bind control source-interface Loopback0** command while there are any active calls or permanent connections in the RMS, the RMS does not apply the command to its running configuration. In this situation, you will encounter a fast busy tone when you call the dial engine directory number. In addition, the Cisco IOS SIP debug logs show a SIP 403 (forbidden) message from the dial engine.

- a. Log in to the RMS.
- b. Enter the following command in privileged mode to make sure that the **bind control source-interface Loopback0** command is applied to the running configuration of the RMS:  
  
Router# **show running-config | include bind control source-interface**
- c. If the **bind control source-interface** command is present in the running configuration, continue to [Step 10](#). If the **bind control source-interface** command is not present in the running configuration, continue to the next step to add the command.
- d. Enter the following command, and view the output that displays in the Total call-legs field, to determine if there are any active calls on the RMS:

Router# **show call active voice brief**

- e. If the Total call-legs field displays zero, continue to [Step g](#). If the field displays a value that is greater than zero, enter voice port configuration mode for the call that is active; then, enter the following command to take the voice port offline and cancel any active voice calls:

**Note**

The following command takes the voice port out of service. Make sure that you enter this command during a maintenance window or other off-peak hours.

Router(config-voiceport)# **shutdown**

- f. Repeat [Step e](#) until you have taken all active calls offline.
- g. Enter the following command in SIP configuration mode to bind the source address of SIP signaling packets to the IP address of the Loopback0 interface:

Router(conf-serv-sip)# **bind control source-interface Loopback0**

- h. To bring the voice ports back online, enter the following command in voice port configuration mode:

Router(config-voiceport)# **no shutdown**

- i. To verify that the output reflects the SIP configuration change that you performed in this procedure, enter the following command:

Router# **show running-config | include bind control source-interface**

- j. To update your configuration on the RMS, enter the following command:

Router# **copy running-config startup-config**

**Note**

For more information about configuring the RMS, refer to the “Configuring the Cisco IPICS RMS Component” chapter in the [Cisco IPICS Server Administration Guide, Release 2.1\(1\)](#).

- Step 10** If you made any changes to the SIP configuration, you must restart the policy engine and the tomcat service by performing the following procedure:

- a. Log in to the Cisco IPICS server by using the root user ID.
- b. To restart the policy engine and the tomcat service, enter the following command:

[root]# **service ipics restart**

**Note**

Be aware that Cisco IPICS cancels all active dial-in or dial-out calls when you enter the **service ipics restart** command.

- Step 11** If you still cannot determine the cause of the dial-in failure, contact your Cisco technical support representative for assistance.

## Troubleshooting Dial-Out Invitation Failures

**Problem** You cannot send dial-out invitations from the Cisco IPICS system.

**Solution** The Cisco IPICS configuration for dial-out invitations or notifications might be incorrect. To check your configuration and fix any problems that you find, perform the following procedure:

### Procedure

- 
- Step 1** Make sure that you have configured an outbound dial number by performing the following steps:
- Navigate to the **Dial Engine > Dial Engine Parameters** window from the Policy Engine tab.
  - Check the Outbound Dial Number field to determine if you have configured an outbound dial number.
  - If a valid number does not exist in the Outbound Dial Number field, create an outbound dial number by following the procedure that is in the “Configuring Dial Engine Parameters” section of the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- Step 2** Check to see if you have ports that are configured for dial-out invitations by navigating to the **Configuration > Ops Views > <opsviewname>** window in the Server tab.
- Step 3** Determine if ports exist for dial-out invitations by checking the following fields in the window:
- Dial ports reserved for dial-in/invite feature
  - Dial ports reserved for dial-in/invite or notifications
- Step 4** If the number in both fields is equal to zero, perform the following steps to add ports for dial-in/invite feature:
- Decrease the number of ports in the **Dial ports reserved for notifications** field.
  - Perform one of the following actions:
    - Add the ports that you removed to the **Dial ports reserved for dial-in/invite feature** field.

- Take no action. Cisco IPICS adds the ports that you removed to the total number of ports that are reserved for dial-in calls, invitations, or notifications.
- 

## Troubleshooting Dial-Out Notification Failures

**Problem** Dial-out notifications do not succeed. You cannot send an e-mail, SMS, pager, or phone message to users.

**Solution** The configuration for dial-out notifications may be incorrect. To check your configuration and fix any problems that you find, perform the following procedure:



### Note

If you are performing dial-out notifications from one ops view to another, see the [“Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views”](#) section on page 3-46.

---

### Procedure

---

- Step 1** If the notification is a dial-out notification, make sure that you have configured an outbound dial number by completing [Step 1](#) in the [“Troubleshooting Dial-Out Invitation Failures”](#) section on page 3-43.
- Step 2** If the notification is an e-mail, SMS or text-based pager notification, make sure that you have configured an SMTP server and a sender e-mail address by performing the following steps:
- Navigate to the **Dial Engine > Dial Engine Parameters** window from the Policy Engine tab.
  - Determine if you have configured an SMTP server for e-mail notifications by checking the Outbound Dial Number field.
  - Determine if you have configured an e-mail address for your server by checking the Sender Email Address field.

- d. Add the SMTP server or sender e-mail address, as required, by following the procedure in the “Configuring Dial Engine Parameters” section in the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- Step 3** Check that ports are configured for dial-out notifications by navigating to the **Configuration > Ops Views > <opsviewname>** window in the Server tab.
- Step 4** Check that ports are configured for dial-out notifications by checking the following fields in the window:
- Dial ports reserved for notifications
  - Dial ports reserved for dial-in/invite or notifications
- Step 5** If the number of dial ports that are reserved for notifications (specified in the **Dial ports reserved for notifications** and **Dial ports reserved for dial-in/invite or notifications** fields) is equal to zero, perform the following steps to add ports for notifications:
- a. Decrease the number of ports in the **Dial ports reserved for dial-in/invite feature** field.
  - b. Perform one of the following actions:
    - Add the ports that you removed to the **Dial ports reserved for dial-in/invite feature** field.
    - Take no action. Cisco IPICS adds the ports that you removed to the total number of ports that are reserved for dial-in calls, invitations, or notifications.
-

## Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views

**Problem** Dial-out invitations and notifications do not succeed from users who belong to different ops views. Users who receive a dial-out message and attempt to authenticate, receive an error message stating that their user ID or Personal Identification Number (PIN) is invalid.

**Solution** If you associate a policy with an ops view, that policy is available only to users who belong to that ops view. Make sure that all users in a policy belong to the same ops view.

You cannot associate users from different ops views to a policy. For example, if a policy belongs to the police ops view, make sure that you associate only users from the police ops view to a policy that contains dial-out invitations and notifications.

**Note**

---

This policy-to-ops-view association information does not apply to the SYSTEM ops view, to which all users belong. For more information about ops views, refer to the “Configuring and Managing Cisco IPICS Operational Views” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

---

## Understanding a PARTIAL\_SERVICE Status For the Dial Engine and Subsystem Manager

**Problem** The dial engine and subsystem manager display a PARTIAL\_SERVICE status. In this release, a fully functional system displays a status of PARTIAL\_SERVICE, which indicates that the system is properly configured and operating normally.

**Solution** If the SIP Subsystem and the IPPE Subsystem display a status of IN\_SERVICE, the dial engine and subsystem manager are operating normally. Check the status of the SIP Subsystem and the IPPE Subsystem by navigating to the **Dial Engine > Control Center > Status** window in the Policy Engine tab.

**Note**

---

The SIP Subsystem status displays as SHUTDOWN until you configure it.

---

## Analyzing a SHUTDOWN Status For the SIP Subsystem


**Problem** After you update your SIP configuration, the SIP Subsystem displays a SHUTDOWN status.

**Solution** This situation may be caused by a SIP misconfiguration or a failure to restart Cisco IPICS after saving a change to the SIP configuration. The SIP Subsystem should display an IN\_SERVICE status if it is properly configured and operational.

To resolve issues with your SIP configuration, perform the following procedure:

### Procedure

- 
- Step 1** Check the status of your SIP configuration by navigating to the **Dial Engine > Control Center > Status** window.
- If the status of the SIP Subsystem displays SHUTDOWN, continue to [Step 2](#).
- Step 2** Make sure that you have configured all of the required fields in the **Dial Engine > SIP Configuration** window. For information about how to configure the SIP Subsystem, refer to the “Configuring the SIP Provider” section in the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- Step 3** If the status of the SIP Subsystem continues to show a status of SHUTDOWN, restart the policy engine and the tomcat service by performing the following steps:
- Log in to the Cisco IPICS server by using the root user ID.
  - To restart the policy engine and the tomcat service, enter the following command:  

```
[root]# service ipics restart
```
-  **Note** You must restart the ipics service after you make any changes to the SIP subsystem configuration.
- 
- Step 4** If the SIP Subsystem continues to show a status of SHUTDOWN, contact your Cisco technical support representative for assistance.
-







## CHAPTER 4

# Troubleshooting Communication, Voice Quality and Other Equipment Issues

---

This chapter describes how to resolve communication and voice quality issues and hardware, firmware, and software issues that you might encounter with other equipment, such as the RMS, and includes the following sections:

- [Troubleshooting Communication Issues, page 4-1](#)
- [Troubleshooting Voice Quality Issues, page 4-7](#)
- [Troubleshooting Equipment Issues, page 4-10](#)
- [Troubleshooting RMS Configuration Issues, page 4-15](#)

## Troubleshooting Communication Issues

This section provides information about communications issues that you may encounter and how to troubleshoot them. The following topics are included:

- [Analyzing Communications Problems Between All Locations on a Channel, page 4-2](#)
- [Troubleshooting Communication Failures Between VTG Participants, page 4-2](#)
- [Resolving Communications Problems For Newly-Added PMC Users on a Channel, page 4-3](#)

- [Removing a Logged-Out PMC User from the Active Users List, page 4-4](#)
- [PMC Users Can Listen to Channels But Cannot Listen to VTGs, page 4-4](#)
- [Configuring the RMS to Eliminate Automatic Channel Deactivation for SIP-Based Remote Connections, page 4-5](#)
- [Eliminating Feedback Noise on VTG, page 4-6](#)
- [Understanding Communication Problems Between Cisco IPICS End Point Devices and Radios That Require a Guard Tone, page 4-6](#)

## Analyzing Communications Problems Between All Locations on a Channel

**Problem** The multicast address for a channel is set to All and the users associated to the channel are from Locations A, B, and C. Users in Locations B and C can converse with each other on the channel, but users in Location A cannot hear the conversation.

**Solution** Although the multicast address for the channel is set to All, the address may not be configured to reach everyone in the domain. You may need to reconfigure the router to include Location A. If the location is configured properly, some other areas to look at include an IP access list that is blocking that channel, a firewall setting, or a multicast address that is not properly configured.

For more information about multicast troubleshooting, refer to the *IP Multicast Troubleshooting Guide* at the following URL:

[http://cisco.com/en/US/tech/tk828/technologies\\_tech\\_note09186a0080094b55.shtml](http://cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080094b55.shtml)

## Troubleshooting Communication Failures Between VTG Participants

**Problem** Participants in a particular VTG cannot communicate with each other.

**Solution** If Protocol Independent Multicast (PIM) on your router is set to sparse mode, this situation might indicate that you have not configured a rendezvous point (RP), or that all RPs are unreachable. If you set the PIM of the router to

sparse mode and do not configure an RP, the router drops the packets and your VTG participants do not hear any audio. To ensure that this problem does not occur, make sure that you configure an RP, or set the router to sparse-dense mode.

For more information about configuring the router, refer to the “Configuring the Cisco IPICS RMS Component” appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*. For more information about multicast troubleshooting, refer to the *IP Multicast Troubleshooting Guide* at the following URL:

[http://cisco.com/en/US/tech/tk828/technologies\\_tech\\_note09186a0080094b55.shtml](http://cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080094b55.shtml)

## Resolving Communications Problems For Newly-Added PMC Users on a Channel

**Problem** Several PMC users have successfully communicated on a channel. However, subsequent PMC users, after successfully logging in to the same location and attempting to activate the same channel, can no longer listen or talk on the channel.

**Solution** The router that the channel uses may not have sufficient digital signal processor (DSP) resources. For this channel to accommodate more PMC users, you may need to add more DSPs. For more information about configuring the RMS, refer to the “Configuring the Cisco IPICS RMS Component” appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

To help calculate the DSPs that you need based on your specific configuration, refer to the *High-Density Packet Voice Digital Signal Processor Modules* document, which is available at the following URL:

<http://www.cisco.com/en/US/products/ps6024/index.html>

## Removing a Logged-Out PMC User from the Active Users List

**Problem** After completing a call, a PMC user logs out of the PMC application. When you view the list of active PMC users in the **Administration > Active Users > PMC** window, the status of the PMC user displays as **Logged-in**.

**Solution** The server did not receive a logout command from the PMC. This situation may occur if the PMC experienced a network connectivity disruption while the PMC user was logging out.

To log out the user and regain RMS and network resources, perform the following procedure:

### Procedure

---

- Step 1** From the Administration Console, navigate to the **Administration > Active Users > PMC** window.
- The PMC Users pane displays the list of active PMC users.
- Step 2** Locate the user ID of the logged-out PMC user.
- Step 3** To manually log out this user, check the check box next to the PMC user ID.
- Step 4** Click **Logout**.
- The PMC user status changes from **Logged-in** to **Logging-out**.
- Step 5** To update the status, click **Refresh**.
- Cisco IPICS removes the user from the list of active users.
- 

## PMC Users Can Listen to Channels But Cannot Listen to VTGs

**Problem** PMC users can remotely join and listen to channels, but when they attempt to listen to a VTG that was created from those channels, the PMC users cannot hear any audio.

**Solution** In Cisco IPICS, an RMS provides support for only one Cisco IPICS location (a Cisco IPICS location is defined as a multicast domain). All of the locations and routers that are configured in the Cisco IPICS system must be able to communicate by using the multicast addresses that have been defined in the

global multicast address pool. All addresses in the multicast pool must be able to reach any RMS, PMC, or Cisco Unified IP Phone that is part of the Cisco IPICS system.

It is important that all RMS components be able to hear or subscribe to all addresses that are defined in the global multicast address pool. Otherwise, an RMS in one location may attempt to provide access to a VTG that is comprised of channels in another, unreachable location. In this case, one RMS cannot listen to the global multicast stream that has been generated by another RMS, so the SIP connection that was created for the user does not work.

To resolve this problem, take either of the following actions:

- From the multicast address pool, remove any multicast addresses that are not reachable by all RMS components, PMC clients, and Cisco Unified IP Phones.
- Deactivate any RMS components that cannot participate in the global multicast address pool. To deactivate an RMS component, navigate to the **Configuration > RMS** window in the Administration Console. Click the RMS that you need to deactivate; then, from the General tab, click **Deactivate**.

## Configuring the RMS to Eliminate Automatic Channel Deactivation for SIP-Based Remote Connections

**Problem** Channels that are activated via a SIP-based remote connection may be deactivated by the RMS if there is no traffic activity after a 30 minute interval. If the PMC user activates several channels, the timing to deactivate is separate for each channel.

**Solution** The PMC automatically reactivates the connection after 30 seconds. Alternatively, you can reactivate the channel by clicking the **Activation** button on the PMC.

To minimize this problem, the system administrator should ensure that the RMS configuration includes the following commands:

```
Router(config)# ip rtcp report interval 5001
```

```
Router(config)# gateway
```

```
Router(config-gateway)# media-inactivity-criteria rtcp
```

Router(config-gateway)# **timer receive-rtcp 5**

For more information about the correct router configuration for Cisco IPICS, refer to the “Configuring the Cisco IPICS RMS Component” appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

**Note**

---

These commands affect the timeouts for all Real-time Transport Protocol (RTP), or voice, traffic on the RMS, not just for Cisco IPICS related communications.

---

## Eliminating Feedback Noise on VTG

**Problem** When a particular user talks in a VTG or channel, there is a continuous feedback noise.

**Solution** Feedback can occur when the audio from the conference plays through the end device of a user who is talking in the conference. For example, you might receive feedback noise if you are listening to a channel or VTG on a handheld radio and talking in that same VTG or channel by using a PMC. The audio from the (handheld radio) speaker feeds back into the microphone (on the PMC). The feedback noise can include sounds, such as metallic echoes or whistling noises.

To avoid feedback, users should turn off radios or speakers in the area in which they communicate on PMC client machines or Cisco Unified IP Phones.

## Understanding Communication Problems Between Cisco IPICS End Point Devices and Radios That Require a Guard Tone

**Problem** When you use a channel that is configured with a radio connection, certain Cisco IPICS end point devices may be able to transmit and receive audio, but the audio may not transmit to radio users. This issue arises when the radio requires a low level guard tone (LLGT).

If the radio requires an LLGT but the LLGT is not statically configured on the LMR gateway, the audio that an IP phone or dial-in/dial-out user sends does not transmit to radio users. In this case, only the PMC, dial-in/dial-out, and other IP phone users can hear the transmission.

If the radio does not require an LLGT, transmissions flow as they would over a channel that does not have an associated radio connection. In this case, all end-users hear the IP phone or dial-in/dial-out user transmissions.

If the LMR gateway includes the LLGT static configuration, or if you have configured the correct guard tone for the channel, the PMC transmission is audible to all end-users.

**Solution** Make sure that you statically configure the LLGT for all radios that require an LLGT.

In addition, note that when you deactivate and then activate (shutdown and no shutdown) an E&M port on the LMR gateway, the router might not process an LLGT while the port is becoming active. This condition can cause short communication outages between radios that require an LLGT and other Cisco IPICS end points.

For additional information about LMRs, refer to the following documentation:

- The “Cisco IPICS LMR Gateway Configurations” chapter of the *[Solution Reference Network Design \(SRND\) for Cisco IPICS, Release 2.1\(1\)](#)*.
- The “Introducing Cisco IPICS” chapter of the *[Cisco IPICS Server Administration Guide, Release 2.1\(1\)](#)*.

## Troubleshooting Voice Quality Issues

This section describes problems that are related to voice quality and includes the following topics:

- [Voice Quality Degrades for PMC, page 4-8](#)
- [Troubleshooting Poor PMC Voice Quality, page 4-8](#)
- [Dial Engine Calls Experience Degraded Voice Quality, page 4-9](#)
- [Resolving Interruption of Voice Communications When You Use VTGs and SIP-Connected PMC Client Machines, page 4-9](#)

## Voice Quality Degrades for PMC

**Problem** Voice quality degrades for PMC users who are connected via multicast or SIP. This problem may correspond to a period of high activity on the router.

**Solution** The PMC client devices may be sending IP packets that are incorrectly marked for voice priority.

For successful voice transmission, each IP packet must be properly marked in the Quality of Service (QoS) Differentiated Service Code Point (DSCP) to ensure the highest priority handling when the packets are transmitted between end points. When devices drop or enqueue packets that are not correctly marked for QoS, voice quality can degrade.

To help resolve this problem, check to make sure that the Microsoft QoS Packet Scheduler is installed on each PMC client machine. For additional details and information about how to install the Microsoft QoS Packet Scheduler, go to <http://www.microsoft.com> and search for QoS Packet Scheduler.

## Troubleshooting Poor PMC Voice Quality

**Problem** Voice quality for PMC users is very poor and some PMC connections are failing.

**Solution** When you configure a channel, you choose the codec, which is the voice-compression algorithm that encodes the voice signal for transmission and then decodes it when the signal reaches the destination. Cisco IPICS allows you to choose between the G.729 codec and G.711 codec.

This problem is most common when you configure a channel to use the G.729 codec, because this codec requires greater DSP resources. G.729 is used for all SIP (remote) connections.

To resolve this problem, ensure that all the DS0 resources in your system are capable of supporting simultaneous G.729 connections.

If the DS0 resources cannot support simultaneous G.729 connections, limit the number of G.729 channels that you use. When it is possible, use G.711 rather than G.729, because G.711 uses fewer DSP resources. For more information about using codecs with Cisco IPICS, refer to the “Choosing a Codec” section in the “Cisco IPICS Infrastructure Considerations” chapter in the *[Solution Reference Network Design \(SRND\) for Cisco IPICS Release 2.1\(1\)](#)*.



You should also restrict the number of remote users who have access to all channels or VTGs, and associate only the required channels to a remote user.

## Dial Engine Calls Experience Degraded Voice Quality

**Problem** Calls to or from the dial engine experience degraded voice quality.

**Solution** The dial engine supports only the G.711 ulaw codec. If your media connections use a different codec, such as G.729, a transcoder must perform the conversion to the G.711 ulaw codec before the voice stream reaches the dial engine. Transcoding can be enabled by using your SIP provider, by configuring an MTP in Cisco Unified Communications Manager, or it can be performed in the Cisco IOS SIP gateway with sufficient DSP resources.

For detailed information about configuring a transcoder in Cisco Unified Communications Manager, release 5.1(2b), refer to the “Transcoder Configuration” chapter in the *Cisco Unified CallManager Administration Guide, Release 5.1(3)* at the following URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)

For more information about Cisco IOS gateway-related features and functionality, refer to the *Cisco Multiservice IP-to-IP Gateway* document at the following URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps5640/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps5640/tsd_products_support_series_home.html)

This document provides information about the Cisco Multiservice IP-to-IP Gateway (IPIPGW), which facilitates connectivity between independent VoIP networks by enabling H.323 VoIP and videoconferencing calls from one IP network to another.

## Resolving Interruption of Voice Communications When You Use VTGs and SIP-Connected PMC Client Machines

**Problem** Voice communications are interrupted when you use VTGs and SIP-connected PMC client machines. Symptoms may include one-way audio transmission, no voice transmission, dropped connections, and poor audio quality.

The **debug vpm signaling** command returns unexpected results (regarding M-lead to E-lead mapping) for voice ports that connect VTGs via T1 loopback ports.

When this problem occurs, Cisco IPICS may generate error messages in the `ipics.log` that appear similar to the following example:

```
2005-11-10 19:25:42,981 [pool-4-thread-1] ERROR IOSRMSCommunicator:433
- 10.32.65.127 getControllers() T1 is missing a required command:
'cablelength short 133ft'
2005-11-10 19:25:42,981 [pool-4-thread-1] ERROR IOSRMSCommunicator:437
- 10.32.65.127 getControllers() T1 controller 1/0/1 UNUSABLE. (Found
24 voice ports)
```

**Solution** Cisco IPICS requires that the **cablelength short** command be configured on all T1 controllers. This command allows you to set a cable length of 133 feet or less for a T1 link on the router.

For detailed RMS configuration information, refer to the “Configuring the Cisco IPICS RMS Component” appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

## Troubleshooting Equipment Issues

The issues that are detailed in this section describe problems that you may encounter with the Cisco IPICS hardware. For issues that relate to communication difficulties, see the “[Troubleshooting Communication Issues](#)” section on [page 4-1](#).

This section includes the following topics:

- [No Power to Cisco Unified IP Phones, page 4-11](#)
- [Analyzing One-Way Audio Issues Between PMC Client Machines and Cisco Unified IP Phones, page 4-12](#)
- [Resolving One-Way Audio Problems on the Cisco Unified IP Phone That Occurs After You Receive or Place a Call, page 4-12](#)
- [Correcting Channel Accessibility Issues with Cisco Unified IP Phones, page 4-13](#)
- [Cisco Unified IP Phone Cannot Access the Cisco IPICS Service After Changing the Server IP Address, page 4-13](#)

- [Resolving Interconnectivity Problems With Cisco Unified Wireless IP Phone 7920, page 4-14](#)
- [Cisco MCS 7825-H2 Server Becomes Inoperable After Removing the Second Hard Drive, page 4-15](#)

## No Power to Cisco Unified IP Phones

**Problem** Cisco Unified IP Phones are not receiving power.

**Solution** When there is no power flowing to the Cisco Unified IP Phones, one of the following circumstances may be true:

- There is no Power over Ethernet (PoE) module in the router.
- The Cisco IOS software version is incorrect.



**Note**

For information about the firmware that Cisco IPICS supports for use with Cisco Unified IP Phones, refer to the [Cisco IPICS Compatibility Matrix](#).

To determine the cause of the power issue, enter the following command on the router:

[router] # **show power**

- If the command returns an “unsupported command” message, the Cisco IOS software version might be incorrect. Installing the correct Cisco IOS version may correct the problem.
- If the command returns information about the power, the cause of the problem might be that there is no PoE module in the router. Installing a PoE module should fix the problem.



**Note**

You can also use an AC/DC adapter to deliver power to the phones. For more information, consult the product documentation for your model of Cisco Unified IP Phone.

## Analyzing One-Way Audio Issues Between PMC Client Machines and Cisco Unified IP Phones

**Problem** Cisco Unified IP Phone users can hear PMC users on a channel, but the PMC users cannot hear the phone users.

**Solution** This situation could occur if the multicast address for a channel is assigned to another resource in your network. Make sure that you assign a unique multicast address to each channel and VTG and that no other resource in your network uses that multicast address. For more information, refer to the “Guidelines for Using IP Multicast Addresses with Cisco IPICS” section in the “Performing Cisco IPICS System Administrator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

## Resolving One-Way Audio Problems on the Cisco Unified IP Phone That Occurs After You Receive or Place a Call

**Problem** After you connect to a channel or VTG by using a Cisco Unified IP Phone, you either receive a call or place an outgoing call. When you try to reconnect to the channel or VTG, you experience one-way audio (users can hear you, but you cannot hear other users).

**Solution** This issue may occur when you use certain models of the Cisco Unified IP Phone. In this case, when the Cisco IPICS multicast voice stream is interrupted by a voice call, the user becomes disconnected from the channel or VTG until the connection is re-enabled.

To resolve this issue, you must reselect the channel or VTG that you were connected to. Or, if you logged out of Cisco IPICS, you must log back in to the system. To reselect the channel or VTG, return to the channel or VTG list by pressing the **Back** softkey. Then, reselect the channel or VTG by pressing the **Select** softkey.

## Correcting Channel Accessibility Issues with Cisco Unified IP Phones

**Problem** A Cisco Unified IP Phone cannot access a channel to which it was associated.

**Solution** The location information may be incorrectly configured. Cisco Unified IP Phones only support multicast connections. To use Cisco Unified IP Phones with Cisco IPICS, you must assign a location that is the same as the dial login default location. The server assigns the configured default location to a phone user when the user logs in to Cisco IPICS. Cisco Unified IP Phone users can access only the associated channels that are assigned to their default location. If the configured default location is the ALL location, Cisco Unified IP Phones users can access only the channels that are assigned to the ALL location.

For more information about managing locations, refer to the “Managing Locations” section in the “Performing Cisco IPICS System Administrator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

## Cisco Unified IP Phone Cannot Access the Cisco IPICS Service After Changing the Server IP Address

**Problem** After you change the server IP address with the **modify\_ip** command, you attempt to log in to the Cisco IPICS service by using a Cisco Unified IP Phone. You select the Cisco IPICS service and enter your digit ID and PIN. The Cisco Unified IP Phone displays an error message or displays a blank prompt.

**Solution** Note the error message that displays on the Cisco Unified IP Phone and perform one of the following actions:

- If the “HTTP error 404” message or a blank prompt displays, the server IP address may not have been updated in Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, and the Cisco IPICS service might be configured with an incorrect server IP address.

**Note**

The Cisco IPICS service does not automatically update its configuration with the new server IP address.

To resolve this problem, configure the Cisco IPICS service so that it uses the new server IP address. For information about configuring your Cisco Unified IP Phone for the Cisco IPICS service, see the “Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device” appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

- If the “Host Not Found” message displays, the Cisco Unified IP Phone firmware may not be compatible with Cisco IPICS. To resolve this problem, refer to the *Cisco IPICS Compatibility Matrix* for the firmware versions that are supported for use with Cisco IPICS, and upgrade the firmware if the current version is not compatible.

For information about using Cisco Unified Communications Manager Administration to upgrade your firmware, refer to the *Cisco Unified Communications Manager Administration Guide* for your applicable version. You can find the Cisco Unified Communications Manager documentation at the following URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)

## Resolving Interconnectivity Problems With Cisco Unified Wireless IP Phone 7920

**Problem** Multiple Cisco Unified Wireless IP Phone 7920 models are connected by an access point. During a conference, the wireless phones can communicate with other devices, but cannot communicate with other Cisco Unified Wireless IP Phone 7920 models.

**Solution** The Cisco Unified Wireless IP Phone 7920 models might be using a downlevel version of firmware. Ensure that your wireless phone is using a version of firmware that is supported by Cisco IPICS. Refer to the *Cisco IPICS Compatibility Matrix* for the supported firmware version.

## Cisco MCS 7825-H2 Server Becomes Inoperable After Removing the Second Hard Drive

**Problem** You remove the second hard drive from a Cisco MCS 7825-H2 server while Cisco IPICS is running, and then reboot the system. Your system becomes inoperable after the reboot.

**Solution** In this situation, the server detects the second hard drive but reflects its status as **degraded** and does not allow the operating system to run from either the CD or the hard drive. To resolve this issue, you must fully reload the server. However, be aware that this procedure results in loss of data.

If you encounter this problem, make sure that you preserve your data by backing up your database before you reboot the server. For more information about backing up your database, see the “Performing Cisco IPICS Database Backup and Restore Operations” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

## Troubleshooting RMS Configuration Issues

The issues in this section describe problems you may encounter with the RMS configuration.

This section includes the following topics:

- [Server Reboots Slowly Following RMS Configuration, page 4-16](#)
- [You Attempt to Deactivate an RMS but its Status Does Not Change, page 4-16](#)
- [VTG Activation Slow or RMS in Unreachable State After RMS Command Prompt Changed, page 4-18](#)
- [RMS Fails or Remains in Unreachable State, page 4-18](#)
- [Newly-Added RMS Does Not Display Loopbacks, page 4-19](#)
- [Router Remains in Unreachable State, page 4-19](#)
- [The Cisco IPICS Server Does Not Recognize All of the T1 Ports on the RMS, page 4-20](#)
- [Router Indicator Lights for the Loopback Are Not Green, page 4-21](#)

- [Voice Loops in VTGs and Router Configuration Shows Incorrect Information, page 4-22](#)
- [Long Delays Between Pressing the PMC PTT Button and Media Establishment, page 4-24](#)

## Server Reboots Slowly Following RMS Configuration

**Problem** You define one or more RMS components and allocate a large number of DS0 voice ports to those components, then reboot the Cisco IPICS server. The server takes an excessively long time to reboot.

**Solution** During a server reboot, the server sends commands to the RMS to verify that the RMS components and DS0s are operational. The server also checks for any changed configuration in the RMS.

If a user adds many DS0s to the RMS, the server has to send numerous commands to the RMS after a reboot; for example, if a user adds 96 DS0s, the server sends between 800 and 1400 commands to the RMS. With higher performance routers, such as the Cisco 3800 series routers, the process of sending and receiving commands may take 10 to 20 seconds. With lower performance routers, such as the Cisco 2800 series routers, this process may take one to two minutes (60 to 120 seconds).

To solve this problem, perform one or more of the following actions:

- Upgrade your router for greater performance.
- Do not load the RMS with an excessive number of controllers and DS0s.

## You Attempt to Deactivate an RMS but its Status Does Not Change

**Problem** You deactivate an RMS, but the status of the RMS displays as Stopping instead of Deactivated.

**Solution** This situation may occur if one or more VTGs are active. Cisco IPICS does not allow you to deactivate an RMS if any active VTGs are using the RMS resources. To resolve this issue, check if you have any active VTGs and deactivate them, if necessary, by performing the following procedure:



### Procedure

---

- Step 1** From the Administration Console, navigate to the **VTG Management > Virtual Talk Groups** window to check the status of the VTGs.
- Step 2** In the Virtual Talk Groups window, read the Status column to check the status of your VTGs.
- The status of this column displays as inactive or active.
- Step 3** For any VTG that displays with an active status, perform the following steps to deactivate the VTG(s):
- Click the link for the VTG name to display the VTG details.
  - Click **Deactivate VTG** to deactivate the VTG.
  - Click **Save**.
- Step 4** After you deactivate all of the active VTGs, check the status of the RMS by navigating to the **Configuration > RMS** window.
- The status of the RMS should display as Deactivated.
- Step 5** If the status of the RMS still displays as Stopping, perform the following steps to activate and deactivate the RMS:
- Navigate to the **Configuration > RMS** window.
  - Click the name of the RMS to select it.
  - Click the **General** tab.
  - To activate the RMS, click **Activate**.
  - To deactivate the RMS, click **Deactivate**.
  - Click **Save**.

The status of the RMS should now display as Deactivated.

---

## VTG Activation Slow or RMS in Unreachable State After RMS Command Prompt Changed

**Problem** You customize the CLI prompt of the RMS with the **prompt** command. After you change the prompt, VTGs are slow to activate, remote user logins are slow or display errors frequently, or the RMS is often in an unreachable state.

**Solution** Changing the prompt on the RMS can cause operations such as VTG activation and deactivation to fail.

Cisco IPICS supports only the default prompts.

To avoid problems, enter the **no prompt** command in global configuration mode to retain the default prompt.

It is also possible that the link between the RMS and the Cisco IPICS server is on a network that has a long packet delay time or is experiencing excessive packet loss. An example of a link with an excessive delay would be a satellite uplink. If possible, use a link that has a lower packet delay time and/or a lower packet loss.

## RMS Fails or Remains in Unreachable State

**Problem** The RMS fails or remains in an unreachable state. When you navigate to the **Serviceability > System Logs** window to check the system logs, the following error message displays in the Recent System Log Entries pane:

```
ERROR IOSRMSCommunicator:...java.net.ConnectException:Connection
refused.
```

**Solution** This problem may occur when multiple Cisco IPICS users log in to the RMS and use all of the available virtual teletype interface (VTY) lines. In this situation, the server cannot communicate with the router.

To verify that all of the VTY lines are in use, log in to the RMS; then, display information about the active VTY lines by entering the following command:

```
Router# show users
```

To clear a VTY line, enter the following command:

```
Router# clear line <line-number>
```

where:

*<line-number>* is the number of the line that you want to clear.

---

## Newly-Added RMS Does Not Display Loopbacks

**Problem** The RMS that you added to Cisco IPICS does not display loopbacks in the **Configuration > RMS > <router-name> Loopbacks** window of the Administration Console.

**Solution** You may have attempted to add an RMS with a partial or unsupported controller configuration. Refer to “Configuring the Cisco IPICS RMS Component” appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for information about connecting and configuring the T1/E1 controllers.

## Router Remains in Unreachable State

**Problem** After updating the login information for an RMS, you cannot access it from the Cisco IPICS server. The **Configuration > RMS** window displays the status of the RMS as Unreachable.

**Solution** You may have activated the RMS with incorrect settings, such as a user name, password, or IP address. This situation causes the RMS to enter an unreachable state, and you cannot fix the incorrect settings or disable the RMS.

This situation can also occur when a formerly operational RMS (with configured loopbacks) already exists in Cisco IPICS and you update the settings to incorrect values.

To resolve the problem, perform the following procedure:

### Procedure

---

- Step 1** Navigate to the **Configuration > RMS** window in the Administration Console. The RMS window displays.
- Step 2** Select the router by checking the check box next to the router name in the Routers pane.
- Step 3** Delete the router configuration from the server by clicking **Delete**.

Cisco IPICS removes the router from the system.

- Step 4** Re-add the router to the configuration by following the procedure in the “Adding an RMS” section in the “Performing Cisco IPICS System Administrator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- 

## The Cisco IPICS Server Does Not Recognize All of the T1 Ports on the RMS

**Problem** The Cisco IPICS server does not recognize all of the DS0s on a T1 controller.

**Solution** Because the Cisco IPICS server does not recognize gaps in the RMS DS0 group configuration, make sure that you always configure sequential DS0 groups on the T1 controller. When DS0 groups are configured out of sequence, the server does not read the configuration that is defined beyond the last DS0 group number in the list.

See [Example 4-1](#) for an example of misconfigured DS0s. If you configure DS0 groups 0 through 2 and then continue with DS0 group 4, the server will only recognize 3 ports on the RMS because DS0 group 3 is not defined. In this situation, the server does not recognize the T1 ports beyond the last sequential configuration (DS0 group 2):

### **Example 4-1 Out of Sequence Configuration**

```
Router(config)#controller T1 1/0
Router(config-controller)#framing esf
Router(config-controller)#clock source internal
Router(config-controller)#linecode b8zs
Router(config-controller)#cablelength short 133
Router(config-controller)#DS0-group 0 timeslots 24 type e&m-lmr
Router(config-controller)#DS0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)#DS0-group 2 timeslots 2 type e&m-lmr
(DS0-group 3 is not configured)
Router(config-controller)#DS0-group 4 timeslots 4 type e&m-lmr
Router(config-controller)#DS0-group 5 timeslots 5 type e&m-lmr
Router(config-controller)#DS0-group 6 timeslots 6 type e&m-lmr
...
```

To resolve this situation for this example, enter the following command on both T1s in the router:

Router(config-controller)# **DS0-group 3 timeslots 3 type e&m-lmr**

After you enter the CLI command on the router, perform the following procedure to merge and save the configuration:

### Procedure

- 
- Step 1** Navigate to **Configuration > RMS** on the Administration Console.  
The **Configuration > RMS** window displays.
- Step 2** Check the check box next to the router to select it.
- Step 3** Click **Configuration > Merge** to merge the configuration.
- Step 4** Click the name of the router to select it.  
The **Configuration > RMS > <rms-name>** window displays.
- Step 5** Click **Save** to update the Cisco IPICS RMS configuration with the changes.
- 

For additional details about configuring the RMS, refer to the “Configuring the Cisco IPICS RMS Component” appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

## Router Indicator Lights for the Loopback Are Not Green

**Problem** After you create a physical loopback on the router, the green Carrier Detect (CD) indicator lights do not illuminate.

**Solution** Check the loopbacks on your router to see if any of the following indicator lights are illuminated, and perform the following actions to correct the problem:

- CD—When this light is green, there are no problems with the loopback
- Alarm Indication (AL)—When this light is red, one of the following problems exist:
  - The cable is not connected

- You have not mapped the pins correctly for a T1. The following is the proper pin configuration on the RJ45 connector:
    - Pins 1 and 2 must be mapped to pins 4 and 5.
    - Pins 4 and 5 must be mapped to pins 1 and 2.
- Loss of Frame (LP)—When this light is yellow, one of the following problems exist:
  - The cable has a loose connection
  - The cable is defective
- Both the AL and CD lights are on
  - The interface is shut down—Enable the interface by entering the following command in interface configuration mode on both ends of the T1 loopback interface:  
Router(config-if)# **no shutdown**
  - The framing is incorrect—Cisco recommends that you use the Extended Super Frame (ESF) framing method on both ends of the loopback.
  - The line code is incorrect—Cisco recommends the B8ZS encoding standard on both ends of the loopback

## Voice Loops in VTGs and Router Configuration Shows Incorrect Information

**Problem** Users experience voice loops (continuous echoes) in VTGs. When you view the configuration by choosing **Show** from the **Configuration** drop-down list box in the **Configuration > RMS** window of the Administration Console, settings for voice ports or dial peers display that are not currently in use.

**Solution** When you add an RMS to a Cisco IPICS system, particularly an RMS that was previously associated with another Cisco IPICS system, you may observe differences between the output that displays with the router **show configuration** command and the configuration that displays when you choose **Show** from the **Configuration** drop-down list box. For example, some of the voice ports may show descriptions that contain an “INUSE” status in the Show Configuration window, even though they are not listed in the loopbacks.

By default, Cisco IPICS polls the RMS every 10 minutes, using the RMS comparator mechanism. The RMS comparator checks the responsiveness of the RMS if there have been any changes made to the configuration. If there have been changes to the RMS configuration and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized.

**Tip**

You can change the polling period by entering a new value in the **RMS Polling Frequency** field in the **Options** window in the Administration drawer. For more information, refer to the “Managing Cisco IPICS Options” section in the “Performing Cisco IPICS System Administrator Tasks” chapter in the *Cisco IPICS System Administration Guide, Release 2.1(1)*.

To manually compare and update without waiting for the polling period, perform the following procedure:

**Procedure**

- 
- Step 1** Navigate to **Configuration > RMS** on the Administration Console.  
The **Configuration > RMS** window displays.
- Step 2** Check the check box next to the router to select it.
- Step 3** Choose **Update** from the **Configuration** drop down list box to update the configuration.

**Note**

Clicking **Update** reconfigures any currently active voice resources on the RMS and may cause a momentary connection loss.

---

## Long Delays Between Pressing the PMC PTT Button and Media Establishment

**Problem** Intermittent delays of varying duration may occur from the time that you press the PMC PTT button to the time that the media is established between the remote PMC and multicast channels.

**Solution** This delay occurs because the RMS cannot perform Reverse Path Forwarding (RPF) checks on multicast RTP packet source addresses. RPF enables more efficient traffic flow and provides loop avoidance by defining the path that multicast packets take between the source and destination addresses.

To resolve this problem, make sure that the IP addresses that you configure for both the Loopback0 and the virtual interfaces (Vifs) are routable; this requirement is mandatory for both interfaces to ensure proper operation with Cisco IPICS. If the IP addresses for either of these interfaces are not routable, your SIP connectivity and/or your Cisco IPICS network connectivity will be affected.

For detailed information about how to configure the RMS, “Configuring the Cisco IPICS RMS Component” appendix in the [Cisco IPICS Server Administration Guide, Release 2.1\(1\)](#).





## CHAPTER 5

# Troubleshooting Tips for the PMC Application

---

This chapter provides information about basic troubleshooting tips and error messages that you may encounter when you use the PMC application.

This chapter includes the following sections:

- [Troubleshooting PMC Application Problems, page 5-1](#)
- [Analyzing PMC Error Conditions, page 5-30](#)

## Troubleshooting PMC Application Problems

The following sections describe how to resolve problems with the PMC application:

- [Resolving PMC Execution Issues, page 5-2](#)
- [Generating a PMC Installation Log File, page 5-3](#)
- [Using the PMC Installer with an Encrypted File System, page 5-5](#)
- [Making PMC Configuration File Changes, page 5-6](#)
- [Using the PMC Optional Settings, page 5-6](#)
- [Resolving Footswitch/USB Device Issues, page 5-7](#)
- [Configuring the Audio Settings, page 5-7](#)
- [Using Cisco Security Agent with the PMC, page 5-9](#)
- [PMC Coexistence with Other Voice Applications, page 5-10](#)

- [Troubleshooting One-Way Audio, page 5-11](#)
- [Troubleshooting Voice Quality Issues, page 5-14](#)
- [Resolving Unknown Publisher Errors with Windows XP SP2, page 5-15](#)
- [Resolving Cisco IPICS Server Administration Console Access Issues with Internet Explorer, page 5-15](#)
- [Troubleshooting PMC Connectivity Issues, page 5-16](#)
- [Resolving Name Resolution Failures, page 5-25](#)
- [Identifying Channel Activation Issues, page 5-26](#)
- [Resolving Codec Mismatch Issues, page 5-27](#)
- [Support for Right-to-Left and Double-Byte Languages, page 5-27](#)
- [PMC Application Caveats, page 5-29](#)

## Resolving PMC Execution Issues

The PMC application allows only one instance of the PMC application to be open on a given PMC client machine. If you launch the PMC, then immediately close it and attempt to relaunch it, the PMC may terminate unexpectedly because the first instance of the PMC has not completed its cleanup procedures. If this situation occurs, wait at least 10 seconds before you restart the PMC.

If you find that you cannot launch the PMC after you have recently closed the application, it may be because the PMC.exe process is still running on the PMC client machine.

To verify that the PMC.exe process is still running and to end the task, if necessary, follow this procedure:

### Procedure

---

**Step 1** On the client machine, press **Ctrl-Alt-Delete** to launch the Windows Task Manager application.

**Step 2** Click **Task Manager**.

Three tabs display on Windows Task Manager: Applications, Processes, and Performance. An additional tab, Networking, displays in the Windows XP Task Manager.

- Step 3** Click the **Processes** tab.
- Step 4** Click **Image Name** to alphabetize the list of running processes.  
Scroll down through this list to look for the PMC.exe process.
- Step 5** Click **PMC.exe** to highlight or right-click **PMC.exe**; then, click **End Process**.  
A warning message displays to ask if you are sure that you want to terminate this process.
- Step 6** Click **Yes**.
- Step 7** Close Windows Task Manager by clicking the “X” in the upper right corner.
- 

**Note**

After you close the PMC, you may need to wait about 30 seconds before you can relaunch the application to provide sufficient time for the PMC to terminate its processes.

---

## Generating a PMC Installation Log File

If you encounter any of the following problems when you try to run the pmcsetup.exe installation file, you can generate a PMC installation log file to help identify and resolve the issue:

- You do not get a response when you attempt to execute the pmcsetup.exe file
- The installation begins to run but it does not complete successfully
- You receive an error that indicates an unsuccessful installation
- You do not see the Cisco IPICS PMC shortcut on the PMC client machine desktop or the Cisco IPICS PMC entry in your programs menu (**Start > Programs > Cisco IPICS > PMC**).

If you experience any of these errors, you can use the following procedure to generate the PMC installation log file from the pmcsetup.exe self-extracting binary file that contains the pmcinst.exe PMC installation file and the pmc.ini file. This log file can provide valuable information to Cisco support personnel to assist in your troubleshooting efforts.

To generate the PMC installation log file, perform the following procedure:

### Procedure

- 
- Step 1** Create a **C:\temp** directory in Windows, if this directory does not already exist.
- Step 2** Use Windows Explorer to navigate to the location where you saved the **pmcsetup.exe** file, as described in the “Downloading and Installing the PMC Application” section in the “Installing and Upgrading the PMC Application” in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.
- Step 3** Locate the **pmcsetup.exe** file in this stored location and click to highlight the file; then, right-click the **pmcsetup.exe** file and click **Copy**.
- Step 4** Use Windows Explorer to navigate to the **C:\temp** directory and right-click in an open area in this directory; then, click **Paste** to copy the **pmcsetup.exe** file to the **C:\temp** directory.



---

**Note** Make sure that the **C:\temp** directory does not contain any versions of the **pmcinst.exe** or **pmc.ini** files. If either file is present, you must rename the existing files or delete them.

---

- Step 5** Open up a command line prompt (**Start > Run > cmd**) on the PMC client machine to access the **C:\temp** directory.
- Step 6** To generate the PMC installation log file, enter the following command from the **C:\temp** directory:

**pmcsetup.exe -log**

The **pmcsetup.log** file appears in the **C:\temp** directory.

If the PMC is already installed on your client machine, you may see a message that asks if you want to upgrade the PMC. Make sure that you click **Yes** to continue.

- Step 7** To close the command line prompt, enter the **exit** command.
- Step 8** After you have created the PMC installation log file, contact your Cisco support personnel for further assistance.
-

## Using the PMC Installer with an Encrypted File System

The PMC installer uses the Temp folder (%temp% environment variable) on your PMC client machine during the installation process. If the Temp folder has been encrypted by using the Encrypted File System (EFS), the PMC installer cannot proceed. In this situation, the PMC installer attempts to use the TMP or the SystemRoot folder to continue with the installation.

If the PMC installation cannot proceed because of encrypted files on the PMC client machine, you can modify the %temp% and %tmp% environment variables to point at nonencrypted folders and then rerun the PMC installation.

To identify the folders that are specified by the %temp% and %tmp% environment variables to determine if they are encrypted, perform the following procedure:

### Procedure

- 
- Step 1** On the PMC client machine, open a command line prompt by choosing **Start > Run** and entering **cmd**.
- A command line window displays.
- Step 2** At the command line, enter the following command:
- ```
C:\ echo %temp%
```
- The location of the TEMP folder displays.
- If the folder that is specified by the %temp% environment variable is encrypted, you can assign the %temp% environment variable to a folder that is not encrypted.
- Step 3** To reassign the %temp% environment variable to a nonencrypted folder, enter the following command:
- ```
C:\ set TEMP=<new location>
```
- where:
- <new location> specifies the new, nonencrypted folder for the %temp% environment variable.
- The new location of the TEMP folder displays.
- Step 4** To reassign the %tmp% environment variable to a nonencrypted folder, enter the following command:
- ```
C:\ set TMP=<new location>
```

where:

<new location> specifies the new, nonencrypted folder for the %tmp% environment variable.

Step 5 Rerun the PMC installation by entering the following command:

C:\ run pmcsetup.exe

Step 6 To close the command line prompt, enter the **exit** command.

For more information about the Encrypted File System, refer to the Microsoft support site at <http://support.microsoft.com/>

Making PMC Configuration File Changes

If you have the PMC application open and you need to make changes to the PMC configuration file, make sure that you close the PMC application before you edit the configuration file on your hard drive; otherwise, the PMC can overwrite your configuration changes. Be sure to save any changes that you make to the configuration file.

Using the PMC Optional Settings

The optional settings menu can aid your troubleshooting efforts by providing access to additional submenus that are not normally viewable or editable, such as the PMC log files. For example, you can manually turn on and turn off logging for individual PMC log files and you can also set debug levels.

These submenu items become available by using the PMC optional settings. Refer to the “Using the Optional Settings Menu” section in the “Configuring the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)* for additional information and caveats about using the PMC optional settings.

**Caution**

You should only use these optional settings to aid troubleshooting and debugging efforts in emergency situations, such as not being able to connect to the server, and as directed by your system administrator or Cisco support personnel. To ensure system integrity, make sure that you contact your system administrator before you use any of these optional settings submenus.

Resolving Footswitch/USB Device Issues

Cisco IPICS supports the use of a device that simulates key down and key up events, such as a footswitch or other USB device. This device must also be capable of simulating key held events as if you were holding down a key on a keyboard.

If you use a footswitch or similar USB device, and you encounter a situation where the All Talk channel button flickers between orange and yellow, you may not have properly configured the device.

Make sure that the device can generate key down events when you hold down the footswitch pedal followed by a key up event when you release the pedal (to simulate pressing and holding a key on a keyboard and then releasing it).

Refer to the product documentation that you received with your USB device for details about how to configure it to properly function with Cisco IPICS.

For more information about using a footswitch or other USB device, refer to the “Using Keyboard Mapping” section in the “Using the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

Configuring the Audio Settings

This section contains information about configuring the audio settings and it includes the following topics:

- [Using a USB DSP Headset with the PMC, page 5-8](#)
- [Checking the Microphone with the PMC, page 5-9](#)

After you have installed the PMC application, check the current settings for the playback and recording audio devices on your client machine to ensure that you are using the preferred or default sound devices with the PMC.

**Tip**

If you change your audio settings while you are running the PMC, you may need to restart the PMC for the changes to become effective.

**Note**

It is very important that you choose the preferred or default sound device option in the Windows audio settings in order to limit echo that can be caused by multiple microphones picking up traffic on the same machine.

For tips about how to ensure the best possible voice quality when you use the PMC, refer to the “Voice Quality Tips” section in the “Installing and Upgrading the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

Using a USB DSP Headset with the PMC

When you use a USB DSP headset (that is, a headset that includes its own sound card) with the Windows operating system, Windows may configure the USB DSP headset as the default speaker and microphone. Therefore, make sure that you connect the USB DSP headset to the PMC client machine before you launch the PMC.

If you launch the PMC after you plug the headset into your PMC client machine, the PMC does not automatically remember the audio setting for the USB DSP headset; instead, the PMC reverts to the Windows operating system’s default audio settings. Refer to the “Using a USB DSP Headset with the PMC” section in the “Installing and Upgrading the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)* for more information about checking and reconfiguring the Windows audio settings for use with a USB DSP headset.

**Note**

If you use the microphone on a USB headset for an extended period of time, your voice may become unintelligible. If this problem occurs, close the PMC and unplug the USB headset from the PMC client machine. Then, plug the USB headset back into the PMC client machine and restart the PMC.

Checking the Microphone with the PMC

You should also check the audio recording and playback capability of the microphone on your PMC client machine by accessing the Microsoft Sound Recorder to record your voice and then listen to the recording. (Make sure that you have an audio input device connected to your machine.)

- Make sure that you use a high-quality microphone with the PMC; otherwise, the Cisco IPICS system may not be able to accurately detect your voice and properly register transmit and/or receive traffic.
- If the Cisco IPICS system cannot detect your voice when you transmit, the system may squelch the transmission; in this situation, another Cisco IPICS user may start speaking over your transmission because your voice cannot be heard and the PMC receive indicator may not display any indication of the transmission.

**Note**

Be aware that if the microphone on the PMC client machine is busy or if it cannot be opened by the PMC for other reasons, you will be able to listen to active conversations but you will not be able to talk.

For detailed information about the audio setting configuration and sound recording capability, refer to the “Configuring the Audio Settings” section, the “Using a USB DSP Headset with the PMC” section, and the “Using the Microphone with the PMC” section in the “Installing and Upgrading the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

Using Cisco Security Agent with the PMC

When you have Cisco Security Agent (CSA) installed on the PMC client machine, be aware that you may be prompted with CSA access permission dialog boxes for various operations that you are trying to perform.

**Note**

Whenever CSA prompts you for permission, while you are performing any operation on the PMC, be sure to always click **Yes** to grant permission and continue with that operation.

CSA may prompt you for permission in the following instances:

- If you are prompted with a CSA access permission dialog box during the PMC installation process, be sure to click **Yes** to grant permission to the PMC installation.
- If you are prompted with a CSA access permission dialog box when you launch a new version of the PMC or after a system reboot, make sure that you click **Yes** to grant permission to allow the PMC to monitor the media device (microphone).

**Note**

If you allow CSA to time-out based on its default value of No after you launch the PMC, the PMC will be able to receive traffic but it will not be able to send traffic; that is, you will still be able to listen to any active conversations but you will not be able to transmit.

- If you are prompted with an access permission dialog box when you activate a channel on the PMC, be sure to click **Yes** to grant permission.
- If you are prompted with an access permission dialog box when you uninstall the PMC, click **Yes** to grant permission.
- If the “Don’t ask me again” check box displays as an option, you may check it to instruct CSA not to prompt you again in the future.

For information about using CSA, refer to the Cisco Security Agent documentation at the following URL:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html

PMC Coexistence with Other Voice Applications

The capability for the PMC application to coexist with other voice applications depends on the operating system that you use.

For example, Windows XP allows multiple applications to run concurrently and open and use the microphone at the same time. Some operating systems, however, do not provide support for this same capability; that is, only one voice application, such as the PMC or another voice application, may be active at the same time on a PMC client machine.

For instance, if you try to open the PMC application while you are running Microsoft NetMeeting conferencing software, the PMC displays an error because it cannot access the media device. In this case, you must first close the NetMeeting application and then launch the PMC. You can then restart NetMeeting.

Troubleshooting One-Way Audio

You may encounter one-way audio issues (such as, you may be able to send audio but you may not be able to hear audio) under various situations when you use the PMC. The following topics provide information about how to resolve these one-way audio issues:

- [Using CLI Commands to Resolve Audio and Headset Issues, page 5-11](#)
- [Resolving IP Address Changes, page 5-13](#)



Note

Be aware that multicast issues may also contribute to problems with one-way audio. For more information, see the “[Troubleshooting Multicast Communications Issues](#)” section on page 5-21.



Tip

Check the network connectivity for your PMC client machine to make sure that you have a valid IP address and that you can connect to the network before you start using the PMC. If you use SIP-based remote connections, make sure that the PMC can establish connectivity to the RMS. (The PMC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS.) For more information, see the “[Resolving IP Address Changes](#)” section on page 5-13.

Using CLI Commands to Resolve Audio and Headset Issues

You can verify and isolate audio issues that you may experience by using CLI command options on the PMC. This section describes the CLI commands that you can use to help resolve audio issues.

Using CLI Commands to Resolve Headset Issues

If you encounter a situation where you cannot hear audio on the PMC, the problem may be due to the headset that you are using. You can verify and isolate one-way audio problems by using CLI command options on the PMC.

Be aware of the following caveats when you use CLI commands:

- Make sure that the PMC to which you are issuing the command is running; the command has no effect if the PMC is not running.
- Issue the command from the Windows command line on the PMC client machine; the command affects only that PMC.

To enter a CLI command on the PMC, follow this procedure:

Procedure

-
- Step 1** On the PMC that has encountered the problem, open the Windows command line by following these steps:
- a. Choose **Start > Run**.
The Windows dialog box displays.
 - b. Enter **cmd** in the Open field.
 - c. Press **Enter** or click **OK**.
The Windows command line window displays.
- Step 2** In the Windows command line window, change the current directory to the folder in which the PMC is installed.
- The following example shows the directory structure in which the PMC folder may appear:
- C:\Program Files\Cisco Systems\Cisco IPICS\PMC**
- Step 3** Enter the desired CLI command and press **Enter**.
- For a description of each CLI command, refer to Chapter 2, “Command Line Interface Commands” in the *Cisco IPICS PMC Command Line Interface, Release 2.1(1)*.
-

Using the CLI Play Command to Resolve One-Way Audio Issues

To verify that the one-way audio problem is not a PMC application issue, you can enter the CLI **play** command from the Windows command line of the PMC.

The play command outputs a wave audio file to the specified PTT channel. This command latches the PMC PTT button, plays the designated wave file, and then unlatches the PTT button. The syntax of the play command appears below:

PMC.EXE -Play *file* [-line #]

- The *file* argument specifies the path and file name of the wave file to play.
- The **-line #** option, where # is a number between 1 and 18, specifies the PTT channel line to which this command applies. (If you omit this option, the command applies to channel 1.)

The following command shows an example of the play command:

PMC.EXE -Play C:\aud1.wav -line 2

In this example, this command plays the aud1.wav file to PTT channel 2.

When you successfully execute this command, you can hear audio from one PMC to another PMC and eliminate the PMC as the source of the one-way audio problem. When this situation occurs, the problem can be isolated to a faulty headset. In that case, replace the headset and try again.



Note

For detailed information about using PMC CLI command options, refer to the [*Cisco IPICS PMC Command Line Interface, Release 2.1\(1\)*](#).

Resolving IP Address Changes

The following section provides information about resolving IP address changes on the PMC client machine; it includes the following topics:

- [Changing IP Addresses on the PMC Client Machine, page 5-14](#)
- [IP Address Change Notifications, page 5-14](#)

Changing IP Addresses on the PMC Client Machine

If you change the IP address on your PMC client machine (for example, when switching from a wired to a wireless network), and the PMC is open, you may encounter one-way audio on the PMC. To resolve this issue, close and then restart the PMC.

If you change the IP address on your PMC client machine when the PMC is not open, the PMC should not be affected by the change. You should always establish network connectivity to make sure that you have a valid IP address before you open the PMC.

IP Address Change Notifications

Under normal conditions, the PMC chooses the first network connection that allows it to communicate with the server. If that network connection becomes unusable, the PMC chooses another network connection for its communications.

Cisco IPICS provides notification to the PMC user when the PMC changes the source IP address that it uses for communications with the server. However, on PMC client machines that include more than one network connection, the PMC may not provide this notification. In these instances, there is no impact to functionality; Cisco IPICS continues to operate normally when notification of the IP address change is not sent to the user.

Troubleshooting Voice Quality Issues

You may encounter voice quality issues, which can arise due to several factors, such as noise and voice distortion.

For detailed information about voice quality problems and symptoms, refer to the [Recognizing and Categorizing Symptoms of Voice Quality Problems](#) documentation, which can be found at the following URL:

http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00801545e4.shtml.

This document categorizes and defines voice quality problem symptoms and may aid your troubleshooting efforts by helping you to identify specific problems through the use of sample sound recordings.

This document also includes a link to the [TAC Case Collection Tool](#), which provides solutions by interactively identifying and troubleshooting common technology or product problems.

You can access the TAC Case Collection Tool at the following URL:
http://www.cisco.com/en/US/customer/support/tsd_tac_case_collection.html

Resolving Unknown Publisher Errors with Windows XP SP2

As part of the browsing security enhancements that were implemented in Microsoft Windows XP Service Pack 2 (SP2), you may encounter an “Unknown Publisher” error when you use the Internet Explorer (IE) browser to download the PMC from the Cisco IPICS server.

This problem may occur when you try to run an executable file or an add-in program that contains an invalid signature and that you downloaded by using the IE version that is installed with Windows XP SP2.

To resolve this issue, Microsoft recommends that you unblock the publisher and then try to save or run the file that you downloaded. Alternatively, you can modify the security settings on your PMC client machine, although this workaround is not recommended.

For detailed information about how to resolve this issue, refer to the Microsoft support site at <http://support.microsoft.com/> and search for Article ID 843022.

Resolving Cisco IPICS Server Administration Console Access Issues with Internet Explorer

For enhanced security on your PMC client machine, Cisco recommends that you review and follow the recommendations that are included in the Windows XP Security Guide. To find this document, refer to the Microsoft support site at <http://support.microsoft.com/> and search for “Windows XP Security Guide.”

When you follow the recommendations that are included in the Windows XP Security Guide and deny all add-ons, except those that are specifically allowed in the add-on list, you may encounter a problem where you cannot access the Cisco IPICS server Administration Console. This issue occurs when you use Internet Explorer from a PC that runs Microsoft Windows XP SP2 and have not enabled the JavaScript GUID in the add-on list.

To resolve this issue and ensure proper operation from Internet Explorer, you must explicitly enable the following JavaScript GUID add-on on your PMC client machine:

- GUID: {F414C260-6AC0-11CF-B6D1-00AA00BBB58} - JavaScript

For detailed information about how to enable this add-on, refer to the Microsoft support site at <http://support.microsoft.com/> and search for Article ID 555235.

Troubleshooting PMC Connectivity Issues

The following topics provide information about troubleshooting PMC connectivity issues:

- [Troubleshooting VPN Connectivity, page 5-16](#)
- [Using the PMC with the Windows XP Firewall, page 5-19](#)
- [Resolving Issues with the Microsoft QoS Packet Scheduler, page 5-20](#)
- [Troubleshooting Multicast Communications Issues, page 5-21](#)
- [Troubleshooting Winsock Corruption Issues, page 5-22](#)
- [Troubleshooting Offline Mode Issues, page 5-23](#)
- [Troubleshooting PMC Connectivity Issues with the RMS, page 5-24](#)
- [Troubleshooting PMC Connectivity Issues with a High Latency, Low Bandwidth Link, page 5-25](#)

Troubleshooting VPN Connectivity

If the Cisco Systems VPN Client is installed on your PMC client machine, you must ensure that the settings for the integrated stateful firewall feature are correctly set to enable PMC remote connectivity. This section includes the following topics to describe the Cisco Systems VPN Client and how to ensure it is correctly set on the PMC client machine:

- [About the VPN Client Stateful Firewall, page 5-17](#)
- [Enabling and Disabling the Stateful Firewall on the PMC Client Machine, page 5-18](#)

Be aware of the following caveats that apply to specific versions of the Cisco Systems VPN Client.

Cisco Systems VPN Client Version Interoperability Caveats

When you use the Cisco Systems VPN Client version 3.6.3(x) with the PMC, the PMC may not be able to detect the IP address and route change after you establish or disconnect a VPN tunnel. This problem occurs when the Cisco Systems VPN Client does not communicate the IP address and route change information to the operating system. When this problem occurs, the channels on the PMC may not be able to receive audio.

To resolve this problem, access the **Settings > Advanced** menu in the PMC application after you have established or disconnected the VPN tunnel on your PMC client machine. When you access this menu, the PMC probes the Cisco Systems VPN Client to determine its activity and tunnel status and, from this menu, it can also detect an IP address change. For more information about the Express menu, refer to the “Configuring the Channels and Advanced Settings” section in the “Configuring the PMC Application” section in the [Cisco IPICS PMC Installation and User Guide, Release 2.1\(1\)](#).

When you use the Cisco VPN Client version 4.0x, the SIP-based remote connection may not become activated. In this situation, you may need to deactivate and then reactivate the channel after you establish the VPN tunnel. To deactivate the channel, click the **Activate** button. Click the **Activate** button again to reactivate the channel.

About the VPN Client Stateful Firewall

The VPN Client integrated stateful firewall provides protection when split tunneling is in effect by safeguarding from Internet attacks while the VPN client is connected to a VPN concentrator through an IPSec tunnel.

When enabled, this “Stateful Firewall (Always On)” feature enforces more robust security by disallowing inbound sessions from all networks, regardless of whether a VPN connection is being used. This firewall is active for both encrypted and unencrypted traffic, except when you use the following protocols:

- Dynamic Host Configuration Protocol (DHCP)—The stateful firewall allows inbound traffic because requests to the DHCP server are sent out one port and responses are received through a different port.
- Encapsulating Security Payload (ESP)—The stateful firewall permits this traffic from the secure gateway because ESP rules are packet filters and not based on sessions.

For more information about exceptions, refer to the release notes for the VPN Client documentation at the following URL:

http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html

Enabling and Disabling the Stateful Firewall on the PMC Client Machine

To ensure PMC connectivity, check the VPN Client Options menu to verify that the “Stateful Firewall (Always On)” feature is disabled. (If a check mark does not appear next to this option, then it is disabled.) The “Stateful Firewall (Always On)” option enables and disables the integrated stateful firewall.



Note

Be sure that the “Stateful Firewall (Always On)” option is not enabled on your PMC client machine. If this option is enabled, you must disable it; otherwise, SIP and multicast connections may not work correctly.



Tip

The “Stateful Firewall (Always on)” feature affects only Internet traffic; when this feature is enabled, it disallows inbound sessions from all networks, regardless of whether a VPN connection is being used. This is true for the VPN Client on any operating system.

To enable or disable the stateful firewall, and manage this setting on your Cisco Systems VPN Client PMC machine, perform the following procedure:

Procedure

- Step 1** Double-click the VPN Client icon to launch the application.
- Step 2** From the VPN Client main dialog box, click the Options drop-down menu button and scroll down to the “Stateful Firewall (Always On)” option. Alternatively, you can right-click the **lock icon** in the system tray and choose **Stateful Firewall**.

**Note**

When the stateful firewall is enabled, a check mark displays next to this option. The stateful firewall feature is disabled by default.

- a. If a check mark appears next to this option, the option is enabled. Click **“Stateful Firewall (Always On)”** to remove the check mark and disable the internal stateful firewall.
- b. If a check mark does not appear next to this option, the option is already disabled. You do not need to take any action.

To view the status of the stateful firewall, right-click the **lock icon** in the system tray during a VPN connection.

Step 3 Close the VPN client.

For additional information about the Cisco Systems VPN Client, refer to the VPN Client documentation for your specific version at the following URL:

http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html

Using the PMC with the Windows XP Firewall

The Microsoft Windows XP operating system includes an integrated firewall to provide additional security. Windows XP and Windows XP Service Pack 1 (SP1) include the Internet Connection Firewall (ICF) while Windows XP SP2 includes the Windows Firewall, as a replacement to the ICF.

For the PMC application to work properly with Windows XP, you may need to modify your firewall settings to ensure that the PMC can send and receive the required protocols.

To modify your firewall settings, perform the following procedure:

Procedure

Step 1 On your Windows XP PMC client machine, navigate to **Start > Control Panel > Network and Internet Connections**.

The Network and Internet Connections window displays.

- Step 2** Click the **Change Windows Firewall settings** link.
The Windows Firewall window displays.
- Step 3** Click the **Exceptions** tab.
A list of programs and services displays.
- Step 4** If you have already installed the PMC, check the **Cisco IPICS PMC** check box to add this program to the list of exceptions in the Windows Firewall; then, proceed to [Step 6](#).
- Step 5** If you have not yet installed the PMC, install and then launch the PMC.
For information about installing and launching the PMC, refer to the “Installing the PMC Application” section and the “Launching the PMC Application” section in the “Installing and Upgrading the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.
- a. After you launch the PMC, a Windows Security Alert displays to inform you that Windows XP has blocked the PMC.
 - b. Click **Unblock** to add this program to the list of exceptions in the Windows Firewall.
- Step 6** Click **OK**.
Windows XP now allows the PMC to function properly.
-

Contact your system administrator if you need assistance with your specific client machine configuration.

For more information about the Windows XP firewall, refer to the Microsoft support site at <http://support.microsoft.com/>

Resolving Issues with the Microsoft QoS Packet Scheduler

If you encounter a situation where the PMC client cannot connect to the Cisco IPICS server, and you do not have a firewall enabled but you can successfully ping the server, the QoS Packet Scheduler may have become corrupted.

To resolve this issue, perform the following steps:

1. Uninstall the PMC application on your PMC client machine. For information about how to uninstall the PMC client, refer to the “Uninstalling the PMC Application” section in the “Installing and Upgrading the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.
2. Uninstall the QoS Packet Scheduler. For additional details and information about how to uninstall the QoS Packet Scheduler, go to <http://www.microsoft.com> and search for “QoS Packet Scheduler.”
3. Reinstall the PMC application on your PMC client machine. For information about how to install the PMC application, refer to the “Installing the PMC Application” section in the “Installing and Upgrading the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

**Note**

The PMC installation process checks to make sure that the QoS Packet Scheduler is installed on your PMC client machine. If the PMC installation process detects that the QoS Packet Scheduler is not installed, it automatically installs the QoS Packet Scheduler on your PMC client machine. Be aware that your user ID must have local administrative rights for this installation to succeed.

4. Check the Windows XP firewall settings and reconfigure, as necessary, to make sure that the PMC displays in the list of exceptions. For detailed information about how to modify the Windows XP firewall setting for use with the PMC, see the “Using the PMC with the Windows XP Firewall” section on page 5-19.

For more information about the QoS Packet Scheduler, refer to the “Voice Quality Tips” section in the “Installing and Upgrading the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

Troubleshooting Multicast Communications Issues

Certain PMC client machines that are running the Windows XP operating system may not be able to send multicast communications because of an issue with the operating system; in these situations, PMC multicast users may experience one-way audio where they can hear, but they may not be heard by, other Cisco IPICS users.

**Tip**

To ensure identification of this specific problem, please check to make sure that the microphone mute options on the headset and in the Windows operating system are not enabled. For more information about using the microphone with the PMC, refer to the “Using the Microphone with the PMC” section in the “Installing and Upgrading the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

This problem with multicast communications may be caused by the network component of the operating system being unable to transmit multicast traffic. Cisco IPICS PMC users who encounter this problem should connect to Cisco IPICS over a unicast connection by choosing the **remote** location from the location selection dialog box. (By choosing the remote location, Cisco IPICS uses SIP-based connectivity for all channels on the PMC.)

To positively identify this problem, use a network packet sniffer as described below:

1. Run the sniffer on the affected PMC client machine and filter for outgoing multicast UDP packets.
2. Then, launch the PMC application and click the **PTT** channel button on one of the channels and speak into the microphone or headset. (The channel highlights and changes color to indicate that you are transmitting traffic.)
3. Observe the sniffer; you will see that no multicast UDP packets are sent from the PMC client machine.

To fully resolve this problem, you must perform a fresh installation of the Windows XP operating system on the PMC client machine.

Troubleshooting Winsock Corruption Issues

If you encounter connectivity problems, such as the inability to send and/or receive IP traffic or if you receive an error when you try to release and renew the IP address on your PMC client machine, you may be experiencing a problem with damaged or corrupted Windows Winsock registry keys.

When the Winsock registry is damaged or corrupted, the PMC client machine may unexpectedly lock up and not accept any additional input.

To fully resolve this problem, you must fix the malfunctioning network components in your Windows installation. To fix the malfunctioning network components, perform one of the following tasks:

- Remove and reinstall the Windows TCP/IP stack
- Issue a command to fix the Winsock corruption (this command is applicable to Windows XP systems only)
- Perform a fresh installation of the Windows operating system

For additional information, access the Microsoft support site at <http://support.microsoft.com> and search for the Microsoft knowledge base article 811259 entitled “How to determine and recover from Winsock2 corruption.” This bulletin contains information about the symptoms and causes of Winsock corruption issues and the procedures that you can follow to resolve these problems.

To help identify problems with the Winsock registry keys and avoid application issues, Cisco recommends that you validate that your Windows Winsock library is not corrupted before you install the PMC application on your client machine.

Troubleshooting Offline Mode Issues

Cisco IPICS allows the PMC to operate in offline mode when the connection to the server has been interrupted so that you can continue to communicate during periods of server downtime.

There are several situations that may cause the PMC to enter offline mode, such as, the inability of the PMC to communicate with the server, networking issues that prevent routing from the PMC client machine to the server, and IE browser settings that cause your PC to work in offline mode.

For detailed information about the situations that apply to offline mode based on interactions between the PMC and the server, refer to the “PMC Offline Mode Caveats” section in the “Using the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

If you encounter a situation where Cisco IPICS returns a message that states that the PMC is in offline mode while the connection to the server is online, check to make sure that your IE browser is not operating in offline mode. To check this setting, choose **File** from the IE browser window. Scroll down to the Work Offline option and make sure that a check mark does not appear next to this option. (If a check mark does not appear next to this option, then it is disabled.)

If a check mark appears next to this option, click **Work Offline** to remove the check mark and disable offline mode.

**Note**

Be sure that the “Work Offline” option in your IE browser settings is not enabled on your PMC client machine. If this option is enabled, you must disable it; otherwise, you may not be able to connect to the server.

Troubleshooting PMC Connectivity Issues with the RMS

To connect the PMC via a SIP-based remote connection, make sure that the PMC can establish connectivity to the RMS. (The PMC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS and configured in the Cisco IPICS server.)

To determine the IP address of the RMS, access the **Settings > Channels** menu in the PMC application. Click a remote connection channel to highlight it; then, scroll through the Channel Properties pane to the SIP Proxy field to find the IP address of the RMS for the associated channel. (If you cannot determine the IP address of the RMS, contact your System Administrator for assistance.)

From the PMC client machine command line interface, enter the following command to ping this IP address to verify connectivity:

C:\>ping <SIP Proxy IP address>

where *SIP Proxy IP address* represents the RMS component.

**Note**

The PMC must be able to establish connectivity to the RMS to enable SIP-based remote connections. Make sure that you can successfully ping this IP address to ensure PMC connectivity to the RMS. If the PMC cannot connect to the RMS, you may experience channel activation issues (such as fast busy) when you attempt to use a SIP-based remote connection.

Troubleshooting PMC Connectivity Issues with a High Latency, Low Bandwidth Link

When you first log in to a PMC that is connected via a high latency and/or low bandwidth link, such as when you use a satellite connection, an error message displays to inform you that the channels are being disabled. This error occurs because of the time delay to connect over this type of link. To recover from this error, click **OK**.

If the Cisco IPICS server times out while it is waiting for a response from one or more resources, the server does not have complete information to send to the PMC. In this case (after about one minute), the server sends an incomplete list of channels to the PMC while it waits for a response.

The server marks each channel that does not respond within the timeout interval as “unavailable” until the operation completes. When this situation occurs, the PMC displays a message that states that the “RMS resources may not be available.”

You do not need to take any action to resolve this issue. After the server completes its tasks, the channels display on the PMC.

**Note**

Be aware that the amount of time that it takes for the server to complete its tasks will vary depending on the amount of latency in the network.

For information about configuring the PMC for use with a high latency and/or low bandwidth link, refer to the “Configuring the Channels Menu Options” section in the “Configuring the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

Resolving Name Resolution Failures

Cisco IPICS requires IP name resolution. An incorrect Domain Name Service (DNS) IP configuration could result in a service outage.

To resolve name resolution failures, consult with your system administrator to confirm IP name resolution within the entire network, which includes local device IP configurations, network-based name resolution systems (such as DNS), and DHCP systems.

Identifying Channel Activation Issues

When you click the **Activate** button on the PMC, the system enters the activating state; that is, the Activate button highlights and the system attempts to connect to the Cisco IPICS server.

- When you click the Activate button immediately after a SIP-based (unicast) channel becomes available on the PMC, you may hear a busy tone if the RMS has not completely configured the line. If you encounter this situation, click the **Activate** button to deactivate the channel; then, wait a few seconds and click **Activate** again to reactivate the channel.

After the connection has been established, the remaining PMC buttons, including the PTT channel button, highlight to indicate that they are in an active state.

- If your ability to transmit on a channel has been disabled by the server, and/or if the channel has been configured by the server as a listen-only channel, the channel will appear dimmed. If the channel has been disabled by the server, you will not be able to activate the channel, as none of the buttons will appear.

If the remaining PMC buttons do not become active, and if you are using a SIP-based connection, one of the following conditions may be occurring:

- Network connectivity issues that prevent connection to the RMS.
- The RMS may be in an offline or invalid state.
- The RMS may be misconfigured in the server.
- The dial peers may not have been configured or the dial peers and/or the voice ports may be misconfigured in the RMS.
- The RMS may not have yet created the dial peers because of a delay between the server configuration and RMS dial peer creation. In this case, you should wait a couple of minutes and then restart the PMC to try again.



Note

When SIP-based remote connections fail, the PMC displays a warning indicator in the form of a yellow triangle next to the channel. This indicator signifies that a problem exists with the remote end (PMC, RMS, or server) and that it may not be able to send or receive traffic. This situation may be caused by a network interruption or reset/restart activity at the remote end. During this period of interruption, the PMC continues to attempt to connect to the remote end. After operations return to normal, the PMC removes the warning indicator from view.

If there is no traffic activity after a 30 minute interval, channels that are activated via a SIP-based remote connection may be deactivated by the system.

- The PMC will automatically reactivate the connection after 30 seconds. Alternatively, you can reactivate the channel by clicking the **Activate** button on the PMC.

Resolving Codec Mismatch Issues

When the protocol type or codec type is misconfigured in the RMS LMR gateway, the PMC has the ability to detect this codec type mismatch (such as G.729 versus G.711) and thereby, preserve system resources and PMC functionality.

If the misconfiguration includes a specific codec type that Cisco IPICS supports (that is, G.729 or G.711), the PMC adapts the codec decoding to enable handling of the different version of that specific codec type. For example, the PMC can adapt to different versions of G.711, such as G.711 ulaw and G.711 alaw, and decode either version automatically to maintain functionality.

If the codec type mismatch is caused by the configuration of an incorrect or unsupported codec type, the PMC will drop the incorrect or unsupported encoded samples because it cannot decode them. In this case, the PMC user will not hear any audio.

For more information about the codecs that Cisco IPICS supports, refer to the “Codec Support” section in the “Understanding PMC Interactions and Supported Features” chapter in the [Cisco IPICS PMC Installation and User Guide, Release 2.1\(1\)](#).

Support for Right-to-Left and Double-Byte Languages



Note

Although this version of Cisco IPICS does not support localization, it does provide support for the PMC to display channel/VTG names that are configured in the server in certain right-to-left (RTL) and double-byte (character-based) languages. This support allows for the input of Arabic and Hebrew characters (RTL languages) and Chinese and Japanese characters (double-byte languages) for names and descriptions in the Cisco IPICS server.

To use a right-to-left language or a double-byte language in Windows XP, you need to configure the operating system to enable support for the specific language that you use.

**Note**

If you try to use the Arabic or Hebrew language without enabling support for RTL, your text will display in reverse.

Procedure

To enable RTL support for the Arabic and Hebrew languages for use with Cisco IPICS, and to enable support for double-byte languages, perform the following procedure:

Procedure:

Step 1 Navigate to **Start > Control Panel > Regional and Language Options**.

The Regional and Language Options dialog box displays. In this dialog box, you can specify options for regional and language settings on your system.

Step 2 Click the **Languages** tab.

- To add support for supplemental languages, check the **Install files for complex script and right-to-left languages (including Thai)** check box in the Supplemental Language Support area.
- To add support for Chinese and Japanese languages, check the **Install Files for East Asian languages** check box.

A pop-up message displays to inform you that the installation of supplemental language support requires a defined amount of available disk space.

Step 3 Click **OK** to accept.

Step 4 From the Regional and Language Options dialog box, click **Apply**; then, click **OK**.

Step 5 If you are prompted, restart your PMC client machine for your changes to become effective.

**Note**

After your PMC client machine restarts, your operating system will be enabled for the languages that you chose.

- Step 6** After the language files have been installed, navigate to Regional and Language Options, as described above, and click the **Details** button in the Text Services and Input Languages pane.
- Step 7** From the Installed Services pane, click **Add**.
The Add Input Language dialog box displays.
- Step 8** From the Input Language drop-down list box, click to select and highlight the input language for one of the supported languages; then, click **OK**.
- Step 9** Check the **Keyboard Layout / IME** check box; from the drop-down list box, choose the keyboard layout to use.
- Step 10** Click **OK**.
The Text Services and Input Languages dialog box displays your selection in the Installed Services pane.
- Step 11** Click **Apply**; then, click **OK**.
- Step 12** Repeat this procedure for each supported language that you want to add.
-

PMC Application Caveats

The following caveats pertain to the PMC application:

- Only one instance of the PMC application can be open and each PMC supports only one user ID login on a given PC at one time.
- A PMC end-user can log in to an unlimited number of different PMC applications at the same time.
- Any number of valid Cisco IPICS users can use the same PMC application, but not concurrently, based on PMC licensing requirements.
- The PMC application can log in to the server that has been configured as the default server and from which the PMC installation file has been downloaded. If the primary server is not accessible, and if there are alternate servers to choose from, you can log in to a different server. For more information about connecting to alternate servers, refer to the “Support for Cisco IPICS Recovery” section in the “Recovering the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

- Refer to the “PMC Usage Guidelines” section in the “Using the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)* for information about using the PMC.
- Refer to the “PMC Offline Mode Caveats” section in the “Using the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)* for information about using the PMC in offline mode.
- Refer to the “Skin Caveats” section in the “Configuring the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)* for information about PMC skin caveats.
- If you use a docking station with your PMC client machine, make sure that you close the PMC application before you undock your PC; otherwise, your PC may become unresponsive and require you to reboot.

Analyzing PMC Error Conditions

This section includes information about identifying and resolving errors that you may encounter when you use the PMC.

In some situations, the PMC may display an error message. In other situations, you may experience certain issues, such as audio quality issues, where a message does not display.

[Table 5-1](#) describes some of these error conditions and audio quality issues and how to resolve them.

Table 5-1 **PMC Error Conditions**

| Problem | Solution |
|--|---|
| <p>You cannot connect to the server. Or, you may see error messages that state you cannot connect to the server but you can connect by using Internet Explorer.</p> | <p>Invalid entries in the <code>pmc.ini</code> file may be the cause of this problem. To check this file, perform the following steps:</p> <ol style="list-style-type: none"> 1. Navigate to C:\Program Files\Cisco Systems\Cisco IPICS\PMC. 2. Search for the pmc.ini file. 3. Right-click pmc.ini and click Open With. 4. Click Notepad; then, click OK. 5. Delete all entries in this file except the following fields: <code>server_host</code>, <code>server_port</code>, and <code>server_port_ssl</code>. 6. Validate that the configured values in these fields are correct. <p>Note Contact your system administrator if you are not sure of these values or if these values are correct and you still cannot connect.</p> |
| <p>You can hear other users but they cannot hear you.</p> | <p>Check your audio settings to make sure that your microphone is not set to mute. Refer to the “Configuring the Audio Settings” section in the “Installing and Upgrading the PMC Application” chapter in the <i>Cisco IPICS PMC Installation and User Guide, Release 2.1(1)</i> for more information about audio settings.</p> <p>Note If you are using a hardware DSP headphone, such as the Plantronics DSP, check to make sure that the external microphone mute button is not switched to the “on” position.</p> |
| <p>When you attempt to download the PMC application from the server, you may receive an error message to inform you that the PMC is not available for download at this time.</p> | <p>This problem may occur if the <code>pmcsetup.exe</code> file was erroneously modified, moved, renamed, or deleted from the server. Contact your system administrator for assistance.</p> |

Table 5-1 **PMC Error Conditions (continued)**

| Problem | Solution |
|---|--|
| When you talk, other users tell you that your voice sounds choppy and breaks up at times during a conversation. | <p>If VAD is enabled, disable the setting in the Channels menu. Refer to the “Configuring the Channels and Advanced Settings” section in the “Configuring the PMC Application” chapter in the Cisco IPICS PMC Installation and User Guide, Release 2.1(1) or more information about VAD.</p> <p>If voice quality still sounds choppy, check the CPU activity on your client machine. If your CPU is overburdened by other programs that are running at the same time, there may insufficient CPU cycles for the PMC to run properly. You can check the CPU usage by opening Windows Task Manager and clicking on the Performance tab.</p> <p>If your CPU utilization appears high, check the applications that are running by clicking the Applications tab and then close any programs that do not need to be open.</p> |
| When you talk, other users tell you that your voice sounds low. | <p>Check the placement of your microphone so that it is positioned between 2 and 6 inches from your mouth. If necessary, reposition the microphone for optimum use.</p> <p>If your microphone gain is set too low, VAD may be interfering with and disabling output; this activity can result in choppy voice quality.</p> <p>Check your audio settings to make sure that the volume is not set too low. If the volume is set low, increase the input gain on your microphone by sliding the bar up on the volume controls to increase the volume.</p> |
| When you talk, other users tell you that they hear a persistent or intermittent noise, such as a hum. | <p>The existence of a persistent or intermittent noise, such as a hum, when you talk may be due to defective headset hardware. In this situation, Cisco recommends that you isolate the source of the audio quality issue by replacing the defective headset with a new, high-quality headset.</p> <p>For more information about voice quality, refer to the “Voice Quality Tips” section in the “Installing and Upgrading the PMC Application” chapter in the Cisco IPICS PMC Installation and User Guide, Release 2.1(1).</p> |

Table 5-1 **PMC Error Conditions (continued)**

| Problem | Solution |
|--|--|
| When you attempt to log in to the PMC, you see an error message that states “invalid user or password.” | <p>This error may display because the password that was entered is incorrect for the specified user name or because the user name does not exist on the Cisco IPICS server.</p> <p>To remedy this situation, log in to the PMC by using a correct user name and password combination. If this action does not resolve the problem, contact your system administrator to request that a new user account be added to the server for the specified user.</p> |
| When you start the PMC after a new installation, the PMC displays an error message to alert you that the PMC cannot register with the Cisco IPICS server and to check your network connection. | <p>Upon initial connection to the server, the PMC must be able to register with the Cisco IPICS server to obtain its unique PMC ID.</p> <p>This error message may display when the PMC tries to connect to a server that is offline and has not yet assigned the PMC ID. When you see this error dialog box, click OK to exit; then, restart the PMC to try again.</p> <p>If the PMC continues to display this error message, contact your system administrator for assistance.</p> |

Table 5-1 **PMC Error Conditions (continued)**

| Problem | Solution |
|---|--|
| The PMC displays a security alert dialog box that prompts you to approve the server certificate. | <p>The PMC has been designed to automatically approve the Cisco IPICS server certificate for secure communications; however, this functionality may not work under certain circumstances. When this functionality does not work properly, the PMC displays a security alert dialog box to inform you that the page requires a secure connection which includes server authentication. To proceed, you must approve the server certificate.</p> <p>On affected PMC client machines, this dialog box appears each time that you run the PMC, once per PMC session (usually during login). When you see this dialog box, you must click Yes to run the PMC. If you click No, the PMC will exit.</p> |
| When you try to launch the PMC, an error message displays because the PMC cannot access the media device. | <p>The PMC application may coexist with other voice applications depending on the operating system that you use. Windows XP allows multiple applications to run concurrently and open and use the microphone at the same time. Other operating systems, however, do not provide support for this same capability.</p> <p>You may encounter this error when you try to open the PMC application while you are running another voice application, such as Microsoft NetMeeting conferencing software, on your PMC client machine. To resolve this issue, close NetMeeting and then launch the PMC. You can then restart NetMeeting.</p> |

Related Topics

To find additional topics that are related to troubleshooting the PMC application, refer to the following sections of the in the [Cisco IPICS PMC Installation and User Guide, Release 2.1\(1\)](#):

- The “Configuring the Audio Settings” section in the “Installing and Upgrading the PMC Application” chapter
- The “Skin Caveats” section in the “Configuring the PMC Application” chapter

- The “Configuring the Channels and Advanced Settings” section in the “Configuring the PMC Application” chapter
- The “Using the Optional Settings Menu” section in the “Configuring the PMC Application” chapter

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.1(1)*
- *Cisco IPICS PMC Command Line Interface, Release 2.1(1)*



CHAPTER 6

Using the Cisco IPICS CLI Tools and Service Commands

This chapter describes the command-line interface (CLI) tools and service commands that are available in Cisco IPICS. You use the CLI tools to fix system problems, and the service commands to start, stop and restart the Cisco IPICS network processes.

This chapter includes the following sections:

- [Understanding the CLI-based Tools, page 6-1](#)
- [Using the CLI-based Tools, page 6-2](#)
- [Configuring and Checking Cisco IPICS Network Processes With Service Commands, page 6-9](#)

Understanding the CLI-based Tools

The CLI-based tools that are bundled with Cisco IPICS allow you enable simplified processing for the following functionality: change the IP address for the server, perform password resets for a subset of users, and enable a user who has been locked.

[Table 6-1](#) lists the Cisco IPICS CLI-based tools.

Table 6-1 *Cisco IPICS CLI-based Tools*

| Log Name | Description |
|-------------------|---|
| enableuser | This tool enables a user who has been disabled, or unlocks a user who has been locked. See the “Unlocking or Enabling a Locked or Disabled User With the enableuser Tool” section on page 6-3 for information about the enableuser tool. |
| modify_ip | This tool changes the IP address for your server. Cisco recommends that you always use the modify_ip tool to change the server IP address; if you do not use this tool, the /etc/hosts file might not get updated with your new IP address, which can cause license and connectivity problems. See the “Changing the Server IP Address With the modify_ip Tool” section on page 6-4 for information about the modify_ip tool. |
| ntpsetup | This tool allows you to configure NTP on the server, enable/disable both the ntpd service and broadcastclient option, check the NTP status, and check NTP activities by viewing the information that is logged in the /var/log/ntpsetup.log file. See the “Configuring NTP on the Cisco IPICS Server with the ntpsetup Tool” section on page 6-5 for information about the ntpsetup tool. |
| reset_pw | This tool resets the ipics password, creates the ipicsadmin and informix passwords, and changes the root password. See the “Resetting, Changing, or Creating a Password With the reset_pw Tool” section on page 6-7 for information about the reset_pw tool. |

Using the CLI-based Tools

This section contains instructions about how to use the CLI-based tools and includes the following topics:

- [Unlocking or Enabling a Locked or Disabled User With the enableuser Tool, page 6-3](#)
- [Changing the Server IP Address With the modify_ip Tool, page 6-4](#)
- [Configuring NTP on the Cisco IPICS Server with the ntpsetup Tool, page 6-5](#)
- [Resetting, Changing, or Creating a Password With the reset_pw Tool, page 6-7](#)

Unlocking or Enabling a Locked or Disabled User With the enableuser Tool

A user can be locked or disabled in the following ways:

- The number of invalid login attempts exceeded the number of maximum attempts, and Cisco IPICS automatically locked the user. For more information, refer to the “Performing Cisco IPICS System Administrator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- A user with Operator or All privileges manually locked or disabled the user. For more information about locking out or disabling a user, refer to the “Performing Cisco IPICS Operator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

When a user is disabled, Cisco IPICS disallows any endpoint devices from logging in to the system; any existing login sessions, such as PMC, dial-in, and Administration Console, are automatically terminated.

When a user is locked, Cisco IPICS disallows any new logins; existing logins continue to work until the user logs out of the system.

Perform the following procedure to unlock or enable a user:

Procedure

-
- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** To log in as the informix user, enter the following command:
- ```
[root]# su - informix
```
- Step 3** To unlock or enable the user, enter the following command:
- ```
[informix]# enableuser <user-id>
```

where:

<user-id> represents the user ID that you would like to unlock or enable.



Note Enter the user ID in all lower case letters.

Changing the Server IP Address With the `modify_ip` Tool

Perform the following procedure to change the IP address of the server:

Procedure

- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** To change the server IP address, enter the following command:

```
[root]# modify_ip
```

The system displays the following text:

Use this tool to facilitate changing the Cisco IPICS server network settings, such as IP address or host name.

To change the current settings, enter the new values below. To accept the existing values without making any changes, press **Enter**.

```
ip address for interface eth0[x.x.x.x]:
```

- Step 3** Enter the IP address for your server; then, press **Enter**.



Note If you have an existing value for this field, or for any of the fields in the following steps, the data in the square brackets displays the current value. To retain the existing value, press **Enter**.

The system displays the following text:

```
Subnet mask for interface eth0[]:
```

- Step 4** Enter the subnet mask for your IP address; then, press **Enter**.
- Step 5** The system displays the following text:

```
default gateway[]:
```

- Step 6** Enter the default gateway for your network; then, press **Enter**.

The system displays the other fields that you configure to ensure network connectivity.

- Step 7** Enter the host name, domain name, primary DNS server and (optional) any secondary DNS servers at the command line when you are prompted. Press **Enter** after each entry.



Note Make sure that you also update your DNS servers if you want to access Cisco IPICS by using the host name.

The system displays the following text:

```
Enter Y to confirm the new settings[No]:
```

- Step 8** Press **Y**; then, press **Enter** to confirm the entries.



Note If you press **No**, or press **Enter** with no text, the system returns you to the beginning of the configuration steps, starting with [Step 3](#).

The system displays the following text:

```
The tool is now ready to modify your system configuration.
After changing the configuration files, the tool will initiate a
system shutdown and restart the server.
If you are using a network connection, your session will be
interrupted and you will need to
reconnect by using the new settings:
```

```
IP Address: 10.1.1.1      Hostname: myhostname
```

```
Enter Y to proceed with these values or N to cancel[N]:
```

- Step 9** Enter **Y**; then, press **Enter** to confirm your choices and reboot the server.
The server reboots and returns you to Login screen.

Configuring NTP on the Cisco IPICS Server with the ntpsetup Tool

This section includes information about how to set up NTP on the server and it includes examples as shown in the [“ntpsetup Command Examples” section on page 6-7](#).

To configure NTP on the server, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 From root, enter the following command:

```
[root]# ntpsetup { [<ntpserver1> [...] <ntpservernn>] } [-b [enable | disable]]
[-s [enable | disable]] [ -c ] [ -h ] }
```

where:

<ntpserver1> through <ntpservernn> represent the IP address or DNS name of one or more NTP servers. If NTP is enabled, Cisco IPICS attempts to use the first NTP server in the list. If Cisco IPICS does not receive NTP broadcast packets from that NTP server, Cisco IPICS attempts to use the next server in the list until a valid NTP server is found.

-b enables or disables the broadcast option. When the broadcast option is enabled, other devices that are in your broadcast domain can use the Cisco IPICS server as an NTP server.

-s enables or disables NTP. When you enable NTP, you must configure at least one NTP server.

-c displays the current NTP status of the server.

-h displays the help screens for this command.



Note

To remove existing NTP server(s), enter the **ntpsetup** command, specify the servers that you want to retain, and omit the server(s) that you want to remove. See the [“ntpsetup Command Examples” section on page 6-7](#) for examples of adding or removing NTP servers.

ntpsetup Command Examples

The following examples show how you can use the **ntpsetup** command:

- The following command enables NTP and specifies ntp1.server.org as the default NTP server and 10.10.10.1 and ntp2.server.org as backup NTP servers:

```
[root]# ntpsetup -s enable ntp1.server.org 10.10.10.1  
ntp2.server.org
```

- The following command removes ntp1.server.org as the default NTP server, specifies 10.10.10.1 as the default NTP server, and retains ntp2.server.org as a backup NTP server:

```
[root]# ntpsetup 10.10.10.1 ntp2.server.org
```

- The following command adds ntp3.server.org as a backup NTP server:

```
[root]# ntpsetup 10.10.10.1 ntp2.server.org ntp3.server.org
```

- The following command allows the Cisco IPICS server to be used as an NTP server for other devices in your broadcast domain:

```
[root]# ntpsetup -b enable
```

Resetting, Changing, or Creating a Password With the reset_pw Tool

If you need to reset the ipics password, create the ipicsadmin or informix passwords, or change the root password, perform the following procedure:

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To reset, change or create a password, enter the following command:

```
[root]# reset_pw
```

The system displays the following text:

```
Select the user name for password reset:
```

- 1) ipics
- 2) ipicsadmin

```

3) informix
4) root
5) quit

```

Step 3 To reset, create or change a password, perform one of the following actions:

- Enter **1** to reset the password for the ipics user.
- Enter **2** to create the password for the ipicsadmin user.
- Enter **3** to create the password for the informix user.
- Enter **4** to change the password for the root user.

The system prompts you to enter a new password for the user.

Step 4 Enter a new password for the user; then, press **Enter**.



Note To ensure a strong password, you must create a password that is at least eight characters long, and includes the following elements:

- At least one lower case letter
- At least one upper case letter
- At least one number
- At least one of the following special characters:
@ [] ^ _ ` ! " # \$ % & ' () * + , - . / : ; { < | = } > ~ ?

The system prompts you to reenter the new password.

Step 5 Reenter the new password for the ipicsadmin or informix user; then, press **Enter**.

Cisco IPICS changes the ipicsadmin or informix user password. To test the new password, log in to the server by using the ipicsadmin or informix user ID.

For more information about the ipicsadmin and informix users, see the “[Glossary](#)” chapter of this document.

Configuring and Checking Cisco IPICS Network Processes With Service Commands

Service commands start, stop or restart network processes, such as the tomcat service or the license manager. Service commands also allow you to check the status of the network processes.

For more information about network processes and the commands that are described in this section, see the [“Troubleshooting Cisco IPICS Network Processes” section on page 2-1](#).

[Table 6-2](#) lists the service commands that you use with Cisco IPICS.

Table 6-2 Cisco IPICS CLI-based Tools

| Log Name | Description |
|--|--|
| service ciscosec {start stop} | This command starts and stops the Cisco Security Agent (CSA). For more information about starting and stopping CSA, see the “Performing CSA Procedures” section on page 2-16 . |
| service ipics {start stop restart status} | This command allows you to start, stop, restart, and check the status of the Cisco IPICS policy engine and the tomcat service. For more information about the policy engine, refer to the “Using the Cisco IPICS Policy Engine” chapter in the Cisco IPICS Server Administration Guide, Release 2.1(1) . |
| service ipics_db {start stop restart status} | This command allows you to start, stop, restart, and check the status of the database server. For more information about the database server, refer to the “Understanding the Cisco IPICS Databases” section in the “Performing Cisco IPICS Database Backup and Restore Operations” chapter in the Cisco IPICS Server Administration Guide, Release 2.1(1) . |
| service ipics_lm {start stop restart status} | This command allows you to start, stop, restart, and check the status of the license manager. For more information about licenses and the license manager, refer to the “Managing Licenses” section in the “Performing Cisco IPICS System Administrator Tasks” chapter in the Cisco IPICS Server Administration Guide, Release 2.1(1) . |

Table 6-2 *Cisco IPICS CLI-based Tools*

| Log Name | Description |
|---|---|
| service ipics_tomcat {start stop restart status} | This command allows you to start, stop, restart, and check the status of the tomcat service. The tomcat service is the web server for Cisco IPICS and enables access to the Administration Console. For more information about the tomcat service, see the “Performing Tomcat Service Procedures” section on page 2-2 . |
| service ippe_dial_engine {start stop status} | This command allows you to start, stop, and check the status of the dial engine. For more information about the dial engine, refer to the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in the Cisco IPICS Server Administration Guide, Release 2.1(1) . |



CHAPTER 7

Understanding the Cisco IPICS Logs

This chapter describes the logs that are available in Cisco IPICS, and how to retrieve and understand the information that is contained in the logs. The logs can help you to troubleshoot problems that may occur with Cisco IPICS and the PMC.

This chapter includes the following sections:

- [Understanding and Locating the Cisco IPICS Log Files, page 7-1](#)
- [Generating and Modifying the PMC Log Levels, page 7-7](#)
- [Checking CSA Logs, page 7-15](#)

Understanding and Locating the Cisco IPICS Log Files

The Cisco IPICS log files contain information that can be used for auditing or tracking the usage of Cisco IPICS. The log files can also help you to determine the root cause of an error.

[Table 7-1](#) lists the Cisco IPICS logs.

Table 7-1 *Cisco IPICS Log Files*

| Log Name | Description |
|--------------|--|
| catalina.out | The catalina.out file contains information about the Cisco IPICS web-based processes, including the tomcat service. The catalina.out file is located in the /root/tomcat/current/logs directory. |

Table 7-1 **Cisco IPICS Log Files (continued)**

| Log Name | Description |
|--------------------------|---|
| Cisco IPICS Activity Log | <p>The Cisco IPICS activity logs store information about activities relating to channels, users, and VTGs.</p> <p>To download and view the information in the activity log in a Microsoft Excel spreadsheet format, log in to the Administration Console as the ipics user, navigate to the Administration > Activity Log Management > Logs window, and click Download Activity Logs. You can change the information that Cisco IPICS saves in the activity log by navigating to Administration > Activity Log Options.</p> <p>For more information about the activity log, refer to the “Performing Cisco IPICS System Administrator Tasks” chapter in the <i>Cisco IPICS Server Administration Guide, Release 2.1(1)</i>.</p> |
| csalog | <p>This file provides CSA startup and shutdown history. The csalog file and the securitylog.txt file contain the logging information for CSA.</p> <p>The csalog file is located in the /var/log directory.</p> |
| CisconnnMIVR nnnn.log | <p>These log files provide you with information about call signaling and Session Initiation Protocol (SIP) information for the policy engine.</p> <p>Cisco IPICS names the initial file Cisco001MIVR0001.log. Subsequent files are named Cisco001MIVR0002.log, Cisco001MIVR0003.log, and so on.</p> <p>You configure the size of each CisconnnMIVRnnnn.log file, the total number of files that Cisco IPICS retains, and the information that Cisco IPICS logs in these files, by navigating to Policy Engine > Dial Engine > Control Center > Tracing in the Administration Console and changing the information in the Trace File Configuration and Trace Settings areas.</p> <p>To download and view the Cisco001MIVR0001.log file, log in to the Administration Console as the ipics user, navigate to the Policy Engine > Dial Engine > Status window and click SIP Subsystem or Policy Engine Subsystem; then, click Cisco001MIVR0001.log. To download and view subsequent log files, navigate to the SIP subsystem or Policy Engine Subsystem window and click on the CisconnnMIVRnnnn.log file that you want to view.</p> <p>The CisconnnMIVRnnnn.log files are located in the /opt/cisco/ippe/log/MIVR directory.</p> |

Table 7-1 *Cisco IPICS Log Files (continued)*

| Log Name | Description |
|----------------------|--|
| CisconnnMVCDnnnn.log | <p>These files provide you with error and status information for the cluster view daemon (CVD) component of the policy engine. The CVD is the node manager for the policy engine and is responsible for managing the startup process for the Cisco IPICS dial engine service.</p> <p>Cisco IPICS names the initial file Cisco001MVCD0001.log. Subsequent files are named Cisco001MVCD0002.log, Cisco001MVCD0003.log, and so on.</p> <p>To download and view the Cisco001MVCD0001.log file, log in to the Administration Console as the ipics user, navigate to the Policy Engine > Control Center > Status > Cluster View Daemon window, and click Cisco001MVCD0001.log. To download and view subsequent log files, navigate to the SIP subsystem or Policy Engine Subsystem window and click on the CisconnnMVCDnnnn.log file that you want to view.</p> <p>The CisconnnMVCDnnnn.log files are located in the /opt/cisco/ippe/log/MVCD directory.</p> |
| db-maintenance.log | <p>The db-maintenance.log file contains records of the database backup and restore operations.</p> <p>To download and view the db-maintenance.log file, log in to the Administration Console as the ipics user, navigate to the Administration > Database Management > Log window and click Download.</p> <p>The db-maintenance.log file is located in the /opt/cisco/ipics/database/logs directory.</p> <p>For more information about the db-maintenance.log file, refer to the “Performing Cisco IPICS Database Backup and Restore Operations” chapter in the <i>Cisco IPICS Server Administration Guide, Release 2.1(1)</i>.</p> |

Table 7-1 *Cisco IPICS Log Files (continued)*

| Log Name | Description |
|------------------------|---|
| dbm_log_archive.log.gz | <p>This file is a compressed file that contains archived data from previous db-maintenance.log daily log files.</p> <p>You can download the dbm_log_archive.log.gz file and save it to your PC by clicking the Download button in the Administration > Database Management > Log window. Once you download the files to your PC, you can view them as a text file.</p> <p>The dbm_log_archive.log.gz file is located in the /opt/cisco/ipics/database/logs directory.</p> <p>For more information about this archive file, refer to the “Performing Cisco IPICS Database Backup and Restore Operations” chapter in the <i>Cisco IPICS Server Administration Guide, Release 2.1(1)</i>.</p> |
| diagnostics.log | <p>The diagnostics.log file contains messages that are related to the database subsystem, and is located in the /opt/cisco/ipics/database/logs directory.</p> |
| driverManagern.log | <p>The driverManager logs contain policy engine-specific information for the media that are associated with each call.</p> <p>To configure the level of detail that the driverManager logs capture, navigate to the Policy Engine > Control Center > Tracing window in the Administration Console and check or uncheck the LIB_MEDIA check boxes.</p> <p>Cisco IPICS sets the size and total number of driverManager files; you cannot change these settings.</p> <p>When a log file reaches the configured maximum size, Cisco IPICS closes that log file and creates a new empty log file, and increments the number of the new log file by one.</p> <p>The driverManagern.log files are located in the /opt/cisco/ippe/log/MIVR directory.</p> |
| install.log | <p>The install.log file shows details of the Cisco IPICS operating system installation, including the packages that were installed and any errors that occurred during the installation.</p> <p>The install.log file is located in the /root directory.</p> |

Table 7-1 *Cisco IPICS Log Files (continued)*

| Log Name | Description |
|-----------------------|---|
| ipics.log | <p>The ipics.log file contains messages regarding all transactions that occur in the Cisco IPICS server. For example, this file contains information about the tomcat service, policy engine entries, or external notifications. The information that is contained in this log file can help you to troubleshoot problems that you might encounter with Cisco IPICS.</p> <p>Each message is marked with a severity level. There are seven severities, from TRACE to FATAL. By default, the ipics.log file captures all logging from the INFO to the FATAL level.</p> <p>You can view recent system logs in the Serviceability > System Logs window of the Administration Console. To download and view the information in the ipics.log, navigate to the Serviceability > System Logs window and click Download.</p> <p>For more information about accessing and downloading the ipics.log file, refer to the “Understanding Cisco IPICS Serviceability and Diagnostic Information” chapter in the <i>Cisco IPICS Server Administration Guide, Release 2.1(1)</i>.</p> <p>The ipics.log file is located in the /root/tomcat/current/logs directory.</p> |
| ipics_audit.log | <p>The ipics_audit.log file records user activity. This activity includes successful and unsuccessful attempts by users to log in to the server, and actions that Cisco IPICS users perform when they are logged in to the Administration Console.</p> <p>The ipics_audit.log file is located in the /root/tomcat/current/logs directory.</p> |
| ipics-install-log.txt | <p>The ipics-install-log.txt file shows details of the Cisco IPICS server software installation, including the packages that were installed, the user names that were created, and any errors that occurred during the installation.</p> <p>The install.log file is located in the /var/opt/CSCOipics/run/yyyymmddhhmmss/ipics-install-log.txt directory, where:</p> <p>yyyymmddhhmmss represents the date and time that you performed the server software installation.</p> |

Table 7-1 *Cisco IPICS Log Files (continued)*

| Log Name | Description |
|---------------|---|
| ipics_pmc.log | <p>This log file collects information for PMC users. Cisco IPICS updates the log file when PMC users log in and log out, or when users update their PMC.</p> <p>The ipics_pmc.log file is located in the /root/tomcat/current/logs directory.</p> <p>Note To retrieve additional PMC data for a user, you can upload logging information from a PMC to the server. For more information, see the “Generating and Modifying the PMC Log Levels” section on page 7-7.</p> |
| ipics_rms.log | <p>The ipics_rms.log file collects log data for the RMS components that are part of the Cisco IPICS system.</p> <p>The ipics_rms.log file is located in the /root/tomcat/current/logs directory.</p> |
| lmgrd.log | <p>The lmgrd.log file contains information regarding Cisco IPICS licenses and the license manager, which is the component that manages the licenses. Cisco IPICS logs any actions that the license manager performs in the lmgrd.log file.</p> <p>You can download and view the lmgrd.log file by accessing the Administration Console as the ipics user, then navigating to the Serviceability > Diagnostics window and clicking Download Diagnostic Results. You receive a zipped file that contains the lmgrd.log and ipics.log files, along with the information that displays in the Diagnostics window.</p> <p>The lmgrd.log file is located in the /opt/cisco/ipics/license/versions/2.1/logs directory.</p> |
| messages | <p>The messages file contains information about the following events:</p> <ul style="list-style-type: none"> • Messages that are related to CSA processing • Users who have logged in to the Cisco IPICS server using SSH • Processes that have stopped or started <p>The messages file is located in the /var/log directory.</p> <p>After seven days, CSA creates a new log and renames the previous log with a numbered extension so that the logs are named messages.0, messages.1, messages.2, and so on.</p> |

Table 7-1 *Cisco IPICS Log Files (continued)*

| Log Name | Description |
|-----------------|---|
| ntpsetup.log | <p>This file records Network Time Protocol (NTP) configuration-related information.</p> <p>The netsetup.log file is located in the /var/log directory.</p> <p>Note You configure NTP by entering the ntpsetup command. For more information, see the “Configuring NTP on the Cisco IPICS Server with the ntpsetup Tool” section on page 6-5.</p> |
| securitylog.txt | <p>This file includes logs of rule violations and other security-related events, and is the primary file that CSA uses for security event logging.</p> <p>The securitylog.txt file is located in the /var/log directory.</p> <p>For more information about the securitylog.txt file, see the “Opening the CSA Security Event Log with CLI Commands” section on page 7-16</p> |
| tacout | <p>The tacout file contains the latest diagnostic summary information for Cisco IPICS.</p> <p>The tacout file is located in the /root/tomcat/current/logs directory.</p> <p>For more information about the tacout file, including instructions for downloading this file, refer to the “Understanding Cisco IPICS Serviceability and Diagnostic Information” chapter of the Cisco IPICS Server Administration Guide, Release 2.1(1).</p> |

Generating and Modifying the PMC Log Levels

The PMC application generates logs that can help you analyze user activity and troubleshoot problems that you may encounter when you use the application. The PMC writes the logs to the hard disk of the PMC client machine, so that the application can continue logging if the communication to the server is disrupted.

Cisco IPICS retrieves logs from the PMC if one of the following conditions are met:

- When you click **Get Logs from PMC** from the **User Management > Users > Username > PMC** tab.

**Note**

You can prevent the server from uploading the logs from the PMC user by navigating to **Settings > Channels** in the PMC application and checking the **Optimize for low bandwidth** check box. You should check this box if you are using the PMC in a low bandwidth, high latency network environment. The PMC still generates logs on the hard drive of the PMC client machine.

- When you set the logs to be uploaded to the Cisco IPICS server automatically when the PMC user logs in, and then out of, a session (this event is called rollover).

Rollover occurs for the Authentication, Channel Statistics and User Interface logs, but not for the Debug Log. In the case of the Debug Log, the file continues to accumulate data until the server requests that the file be uploaded. For more information about a rollover occurrence, refer to the “Using the PMC Application Logs” chapter in the [Cisco IPICS PMC Installation and User Guide, Release 2.1\(1\)](#).

Users can modify the PMC logs in the following ways:

- The PMC user can adjust settings within the PMC application. For more information about adjusting settings in the PMC application, refer to the “Using the PMC Application Logs” chapter in the [Cisco IPICS PMC Installation and User Guide, Release 2.1\(1\)](#).
- From the Administration Console, the Cisco IPICS operator can modify the log settings in the **User Management > Users > Username > PMC** tab. See the “Performing Cisco IPICS Operator Tasks” chapter in the [Cisco IPICS Server Administration Guide, Release 2.1\(1\)](#) for more information about setting and modifying the log settings.

For a list of the log files and their descriptions, refer to the “Using the PMC Application Logs” chapter in the [Cisco IPICS PMC Installation and User Guide, Release 2.1\(1\)](#).

You can download activity logs for PMC users in the **Administration > Activity Log Management > Logs** tab of the Administration Console. The information that you download includes details about user associations to channels and VTGs, channel activation activities, and conference participation. You configure the activity logs to capture the PMC information in the **Administration > Activity**

Log Options window. For information about the activity logs, refer to the “Performing Cisco IPICS System Administrator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

This section contains the following topics:

- [Understanding PMC Debug Log Information, page 7-9](#)
- [Using the Debugging Log Level, page 7-10](#)

Understanding PMC Debug Log Information

Cisco IPICS organizes the DebugLog.txt data fields into three categories: User Interface, Signaling, and Media. These data fields are then divided into three logging levels, so that you can capture more precisely the debugging information that you need. The Debug Log categories contain the following information:

- **User Interface**—These fields provide information about aspects of the user interface for the PMC. The category includes everything that the user can see on the PMC application, such as the buttons and volume controls. The User Interface category also includes information for debugging communication problems with the Cisco IPICS server.

[Table 7-2](#) describes the information that Cisco IPICS gathers, by log level:

Table 7-2 User Interface Log Levels

| Logging Level | Purpose |
|---------------|--|
| Low | <p>Cisco IPICS retrieves information for the following problems at this logging level:</p> <ul style="list-style-type: none"> • The user cannot log in • The user has difficulty activating channels • The user cannot close the PMC • The PMC unexpectedly goes into offline mode • The server is reporting errors |
| Medium | Cisco IPICS reports information that can help translate XML communication from the server. |
| High | Cisco IPICS gathers information regarding authentication, the GUI, and the PMC server update function. |

- **Signaling**—The Signaling category includes fields that provide information about the starting and stopping of voice channels. You would turn Signaling on when a user is not able to activate or deactivate a PMC channel.

[Table 7-3](#) describes the information that Cisco IPICS reports by signaling levels.

Table 7-3 **Signaling Log Levels**

| Logging Level | Purpose |
|----------------|--|
| Low and Medium | Messages at these log levels describe issues with the high level state machines. |
| High | Messages at this level report issues with SIP messaging. |

- **Media**—These fields involve items related to the voice stream, such as the packets and the codecs that handle the data between end points. You would use Media information to diagnose any voice quality problem.

[Table 7-4](#) describes the type of information you can gather with the Media log levels.

Table 7-4 **Media Log Levels**

| Logging Level | Purpose |
|---------------|---|
| Low | This information provides receive (RX) and transmit (TX) networking statistics. |
| Medium | This information can help you diagnose audio mixing issues, such as the combining of audio signals in a channel or VTG. |
| High | This information provides you with information regarding the conversion of audio using audio codecs. |

Using the Debugging Log Level

When you choose to begin logging debug information for a PMC user, you select one or more of the information categories, each of which includes a list of debugging fields. You choose the category and logging level as it corresponds to the fields that you want to capture in the log.

Table 7-5 shows the fields that are included in each logging level.

The log levels for each category are cumulative. If you choose the Medium level for a category, the PMC writes Low- and Medium-level logs into the DebugLog.txt file. When you set the logging to High, you capture all the fields for that category.

**Tip**

Always start debugging by collecting Low-level log data, which may provide all of the data that you require. Using this setting allows you to gather several days of log activity without filling the hard disk of the PMC client machine. If you cannot locate the cause of the problem, you can next set the logging to Medium or High.

Use the High level only for short durations. If you use the High level, you should closely monitor the hard drive of the user PMC client machine so that the High-level logs do not overwhelm the client hard drive or degrade the performance of the PMC.

**Caution**

Because of the large amount of information that the system collects and generates when you set all of the debug options, Cisco recommends that you use debug logging only to isolate specific problems. When you complete your debugging tasks, be sure to turn off debug logging by clearing the debug log.

Table 7-5 lists the debug categories, and the fields and log levels that are associated with each category.

Table 7-5 **Debug Log Fields and Log Levels**

| Category | Field | Log Level |
|----------------|-----------------------------|-----------|
| User Interface | channel-activation-debug | Low |
| | error | |
| | exit-debug | |
| | sending-source-debug | |
| | sock-init-cleanup | |
| | xml-events | Medium |
| | xml-post | |
| | xml-vars | |
| | Auth | High |
| | critical-section-tune-debug | |
| | download-debug | |
| | gui-debug | |
| | server-task-debug | |
| | server-verbose | |
| | xml-deck | |

Table 7-5 *Debug Log Fields and Log Levels (continued)*

| Category | Field | Log Level |
|-----------|---------------------------|-----------|
| Signaling | cc | Low |
| | fim | |
| | fsm | |
| | gsm | |
| | lsm | |
| | multicast-signaling-debug | |
| | sip-reg-state | |
| | sip-state | |
| | vcm | |
| | sip-task | Medium |
| | sip-trx | |
| | Auth | High |
| | cc-msg | |
| | sip-messages | |

Table 7-5 **Debug Log Fields and Log Levels (continued)**

| Category | Field | Log Level |
|----------|------------------------|-----------|
| Media | AMuteTrans | Low |
| | AudioSink | |
| | AudioSource | |
| | MediaStream | |
| | OpenALAudioSink | |
| | RTPAudioSink | |
| | RTPAudioSockets | |
| | RTPAudioSource | |
| | RTPAudioStream | |
| | RTPJitterBuf | |
| | sock-init-Cleanup | |
| | WaveAudioSource | |
| | WaveFileSource | |
| | RxStats | |
| | TxStats | |
| Media | ACMTrans | Medium |
| | ASL | |
| | AudioBufferAndPlayback | |
| | dsp | |
| | FilePlay | |
| | PCMMixer | |
| | PCMVolTrans | |
| | PCMVolumeMax | |
| | RTPAudioStreamMgr | |
| | RxDetailStats | |
| | VAD | |

Table 7-5 *Debug Log Fields and Log Levels (continued)*

| Category | Field | Log Level |
|----------|----------------------|-----------|
| Media | AudioDump | High |
| | AudioSamp | |
| | AudioSampLost | |
| | AudioSampMgr | |
| | AudioTrans | |
| | AutomaticGainControl | |
| | dtmf | |
| | FIRTrans | |
| | FSAudioBuf | |
| | G7112PCMTrans | |
| | G7232PCMTrans | |
| | G729A2PCMTrans | |
| | Limiter | |
| | PCM2G711Trans | |
| | PCM2G723Trans | |
| | PCM2G729ATrans | |
| | RTCPPacket | |
| | TimeSample | |
| | TimeRxSample | |
| | TimeTxSample | |

Checking CSA Logs

If CSA denies a system action, the process generates a message that you can access in one of the following ways:

- You can open the CSA Utility to view the messages in the Message pane

- You can view the Security Events Log, which includes all security events that have occurred on the system
- You can navigate to the `/var/log` directory, and view the current and archived CSA logs

This section includes the following topics:

- [Viewing the CSA Messages from the CSA Utility, page 7-16](#)
- [Opening the CSA Security Event Log with CLI Commands, page 7-16](#)

Viewing the CSA Messages from the CSA Utility

To view status messages in the CSA utility, perform the following procedure:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Double-click the CSA tray icon (the red flag) to open the CSA Utility. The CSA Utility displays. |
| Step 2 | To access the Security Logs, click Messages . Status messages display in the Messages pane. |
| Step 3 | To view the CSA log, click View Log . The current Security Events Log displays in a text viewer window. |
-

Opening the CSA Security Event Log with CLI Commands

The `/var/log` directory in the Cisco IPICS server contains the current and archived CSA logs.

The file name of the log that contains security events is **securitylog.txt**. When the securitylog.txt file reaches a size of 100 MB, CSA creates a new log, and archives and renames the previous log file. Archived log files are named **securitylog-yyyymmdd-hhmm.txt**,

where:

yyyymmdd-hhmm is the date that CSA archived the log file.

To view the securitylog.txt file by using CLI commands, perform the following procedure:

Procedure

- Step 1** Log in to the Cisco IPICS server by using the root user ID.
- Step 2** To navigate to the **/var/log** directory, enter the following command:
- ```
[root] #cd /var/log
```
- Step 3** To view the security event log files in the directory, enter the following command:
- ```
[root] #ls -al securitylog*
```
- Files that begin with the name securitylog display.
- Step 4** To view the contents of a log file, enter the following command:
- ```
[root] #cat securitylog[-yyyymmdd-hhmm].txt
```

Where:

*yyyymmdd-hhmm* is the date of the archived log file.

---

For information about the messages that appear in the CSA logs, refer to the CSA documentation at this URL:

[http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html)







## GLOSSARY

---

### A

|                                  |                                                                                                                                                                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>activated</b>                 | A VTG state that indicates that the SIP (unicast) line or multicast line is fully operational. <b>The PTT and volume indicators appear highlighted.</b>                                                                 |
| <b>activating</b>                | A VTG state that becomes effective when the Activate button is clicked. The Activate button appears highlighted while the other PMC buttons remain in an inactive state as the system attempts to activate and connect. |
| <b>activation button</b>         | This button toggles activate and deactivate functionality on the PMC. Click this button on the PMC to activate a channel (to call out); click it again to deactivate the channel.                                       |
| <b>active virtual talk group</b> | A virtual talk group (VTG) becomes active when Cisco IPICS commits global resources, such as a multicast address and any necessary dial-in peers, so that the participants in the VTG can communicate with each other.  |
| <b>Administration Console</b>    | The graphical user interface (GUI) in the Cisco IPICS server software through which authorized Cisco IPICS users can manage and configure Cisco IPICS resources, events and VTGs.                                       |
| <b>autonomous system</b>         | A radio system under one administrative control; also known as a management domain. This system is usually mapped to an agency.                                                                                         |

---

### B

|                               |                                                                                                                                                                                                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>backward compatibility</b> | The ability of newer radio equipment to operate within an older system infrastructure or to directly intercommunicate with an older radio unit. The term usually applies to digital radios that are also capable of analog signal transmission. |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth</b>    | The difference between the highest and lowest frequencies that are available for network signals. The term also describes the rated throughput capacity of a specific network medium or protocol. Bandwidth specifies the frequency range that is necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 7 kHz of bandwidth and data traffic typically requires approximately 50 kHz of bandwidth. |
| <b>base station</b> | A land station in the land mobile radio service. In the personal communication service, the common name for all the radio equipment that is located at one fixed location and used for serving one or several calls.                                                                                                                                                                                                                                                 |

---

## C

|                        |                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CAI</b>             | common air interface. The standard for the digital wireless communications medium that is employed for P25-compliant radio systems and equipment. The standard for P25 Phase I incorporates Frequency Division Multiple Access (FDMA) technology.                                                                                                                                        |
| <b>call</b>            | Radio terminology that defines a call as beginning at the moment that you press the transmit key and concluding when you release the transmit key. The term “per call” implies that some form of control causes the radio to select a specific frequency before it transmits audio. Some radios may be configured to automatically return to a predefined RF channel when the call ends. |
| <b>call delay</b>      | The delay that occurs when there is no idle channel or facility available to immediately process a call that arrives at an automatic switching device.                                                                                                                                                                                                                                   |
| <b>call setup time</b> | The time that is required to establish a circuit-switched call between users or terminals.                                                                                                                                                                                                                                                                                               |
| <b>carrier</b>         | A wave that is suitable for modulation by an information-bearing signal.                                                                                                                                                                                                                                                                                                                 |
| <b>CAS</b>             | channel associated signaling. The transmission of signaling information within the voice channel. CAS signaling often is referred to as robbed-bit signaling because user bandwidth is being robbed by the network for other purposes.                                                                                                                                                   |

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>channel</b>                                            | A communication path that is wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments. There are many different types of channels in Cisco IPICS, including direct dial, 2-way, VTGs, and radio channels. Channels can be dynamically or statically allocated. Channels may have one or more channel connections that define the source for the channel. <i>See</i> PTT channel. |
| <b>channel capacity</b>                                   | The maximum possible information transfer rate through a channel, subject to specified constraints.                                                                                                                                                                                                                                                                                                                                                      |
| <b>channel connection</b>                                 | One or more methods by which a content stream can be obtained. For instance, a particular channel may be found on several different multicast addresses in different locations and also on several different radios at different locations.                                                                                                                                                                                                              |
| <b>channel folder</b>                                     | A logical grouping of channels                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>channel select check box</b>                           | Provides the ability to select or deselect the specified channel on the PMC for audio transmission.                                                                                                                                                                                                                                                                                                                                                      |
| <b>channel spacing</b>                                    | The distance from the center of one channel to the center of the next-adjacent-channel. Typically measured in kilohertz.                                                                                                                                                                                                                                                                                                                                 |
| <b>Cisco Unified Communications Manager (CallManager)</b> | The software-based call-processing component of the Cisco IP telephony solution. Cisco Unified Communications Manager (CallManager) extends enterprise telephony features and functions to packet telephony network devices, such as Cisco Unified IP Phones, media processing devices, VoIP gateways, and multimedia applications.                                                                                                                      |
| <b>Cisco IPICS</b>                                        | Cisco IP Interoperability and Collaboration System. The Cisco IPICS system provides an IP standards-based solution for voice interoperability by interconnecting voice channels, talk groups, and VTGs to bridge communications amongst disparate systems.                                                                                                                                                                                               |
| <b>Cisco IPICS policy engine</b>                          | Integrated with the Cisco IPICS server, this component enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.                                                                                                                                                                                                                                                                      |

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cisco IPICS server</b>        | Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Linux operating system on selected Cisco Media Convergence Server (MCS) platforms. The server software includes an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. The server also includes the Cisco IPICS policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications. |
| <b>Cisco Unified IP Phone</b>    | A full-featured telephone that provides voice communication over an IP network. A user can participate in a PTT channel or VTG by using a Cisco Unified IP Phone as a PTT device.                                                                                                                                                                                                                                                                                                                                                             |
| <b>Cisco Security Agent</b>      | Provides threat protection for server and desktop computing systems (endpoints) by identifying, preventing, and eliminating known and unknown security threats.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CLI</b>                       | command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments.                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>codec</b>                     | <p>coder-decoder.</p> <ol style="list-style-type: none"><li>1. Integrated circuit device that typically uses pulse code modulation to transform analog signals into a digital bit stream and digital signals back into analog signals.</li><li>2. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm that is used to compress/decompress speech or audio signals.</li></ol>                                                                                                                               |
| <b>conference of conferences</b> | A conference that consists of two or more VTGs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>conventional radio system</b> | A non-trunked system that is similar to telephone party-line in that the user determines availability by listening for an open channel.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>COR</b>                       | carrier operated relay. An electrical signal that is used to signal when a radio is receiving traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>coverage</b>                  | In radio communications, the geographical area that is within the range of, or that is covered by, a wireless radio system to enable service for radio communications. Also referred to as service delivery area.                                                                                                                                                                                                                                                                                                                             |

---

**D**

|                                     |                                                                                                                                                                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>delay time</b>                   | The sum of waiting time and service time in a queue.                                                                                                                                                                                                    |
| <b>decrypt</b>                      | Cryptographically restore ciphertext to the plaintext form it had before encryption.                                                                                                                                                                    |
| <b>decryption</b>                   | Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state.                                                                                                                       |
| <b>dial engine scripts</b>          | Scripts that the Cisco IPICS dial engine executes to provide the telephony user interface (TUI) for interaction with incoming and outgoing phone calls.                                                                                                 |
| <b>dial-in</b>                      | A phone call that is dialed in to the policy engine.                                                                                                                                                                                                    |
| <b>dial-in floor control</b>        | A feature that allows one dial-in user, at a time, to talk in a VTG or a channel. The telephony user interface provides this dial-in floor control feature to support dial-in users. It does not provide support for floor control for other PTT users. |
| <b>dial number</b>                  | The phone number that is used by the policy engine and the SIP provider and configured in the Dial Information pane in the Ops Views window. Dialing this number provides user access to the telephony user interface.                                  |
| <b>dial out invite</b>              | <p>An action that invites selected user(s) to the selected VTG.</p> <p>A phone call that is dialed out by the policy engine to a phone user to invite the user in to a talk group.</p>                                                                  |
| <b>dial peer</b>                    | Addressable call endpoint. In Voice over IP, there are two kinds of dial peers: POTS and VoIP.                                                                                                                                                          |
| <b>digit ID</b>                     | A numeric identifier that is chosen by a Cisco IPICS user and stored in the user profile. Cisco IPICS uses this ID and a numeric password to authenticate a Cisco Unified IP Phone user.                                                                |
| <b>digital modulation technique</b> | A technique for placing a digital data sequence on a carrier signal for subsequent transmission through a channel.                                                                                                                                      |
| <b>discrete tone</b>                | Any tone that is sent without any summed or added tone. For example, adding a function tone with a low level guard tone may impact the recognition of the function tone. Contrast with mixed tones.                                                     |

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dispatcher</b>                              | The Cisco IPICS dispatcher is responsible for setting up the VTGs, activating the VTGs to begin conferences, and adding and/or removing participants in inactive VTG and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute PMC users, as necessary, and manages policies, which activate/deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges. |
| <b>DS0</b>                                     | digital service zero (0). Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX.                                                                                                                                                                                                                                                                                                                           |
| <b>DTMF</b>                                    | dual tone multi-frequency. The signal to the phone company that you generate when you press keys on a telephone keypad. With DTMF, each key that you press on your phone (0 through 9, ‘*’ and ‘#’) generates two tones of specific frequencies; one tone is generated from a high frequency group of tones and the other from a low frequency group. Voice gateways often strip these inband tones and present them out-of-band in SIP, H.323, or other messages.                                                                  |
| <b>dynamic radio channel (dynamic control)</b> | The controls that are used to preset radio characteristics so that channels are available to clients.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>dynamic regrouping</b>                      | A trunking system feature that allows multiple radios to be placed upon a specific talk group without manual manipulation of the programming of the radios. Dynamic regrouping is initiated through a system control console and transmitted to the radio via the trunking systems control channel.                                                                                                                                                                                                                                 |

---

## E

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E &amp; M</b>  | <p>receive and transmit (or ear and mouth). As the analog interface between a radio and the LMR gateway, the E&amp;M interface provides voice signals from radio channels, which are then mapped to IP multicast or unicast. The E&amp;M interface provides the most common form of analog trunking.</p> <ol style="list-style-type: none"><li>1. Trunking arrangement that is generally used for two-way switch-to-switch or switch-to-network connections. Cisco's analog E&amp;M interface is an RJ-48 connector that allows connections to PBX trunk lines (tie lines). E&amp;M also is available on E1 and T1 digital interfaces.</li><li>2. A type of signaling that is traditionally used in the telecommunications industry. Indicates the use of a handset that corresponds to the ear (receiving) and mouth (transmitting) component of a telephone.</li></ol> |
| <b>e-lead</b>     | The ear portion of the E & M interface. The e-lead is the receive path of the LMR gateway.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>encipher</b>   | To convert plain text into an unintelligible form by using a cipher.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>encode</b>     | To modify information into the required transmission format.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>encryption</b> | Application of a specific algorithm so as to alter the appearance of data and make it incomprehensible to unauthorized users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>event</b>      | An active VTG in the Cisco IPICS solution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

---

## F

|             |                                                                                                                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FDM</b>  | frequency-division multiplexing. Technique whereby information from multiple channels can be allocated bandwidth on a single wire based on frequency.                                                                    |
| <b>FDMA</b> | frequency-division multiple access. A channel access method in which different conversations are separated onto different frequencies. FDMA is employed in narrowest bandwidth and multiple-licensed channel operations. |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FLEXIm</b>               | Cisco software that enforces licensing on certain systems; FLEXIm ensures that Cisco IPICS software will work only on the supported and licensed hardware.                                                                                                                                                                                                                                                                                   |
| <b>floor control</b>        | The standard mechanism for Push-to-Talk speaker arbitration.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>frame</b>                | A logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and the trailer, used for synchronization and error control, that surround the user data contained in the unit. The terms cell, datagram, message, packet, and segment also describe logical information groupings at various layers of the OSI reference model.                                                     |
| <b>frequency</b>            | For a periodic function, frequency represents the number of cycles or events per unit of time. Frequency is used in several different contexts. For example, transmission frequency (the band on which the radio sends signals) or the frequency of an audible signal measured in hertz (Hz). All tone control operations require audible tones that fall within a narrow band of a specific frequency and at a specific volume (amplitude). |
| <b>frequency assignment</b> | Assignment that is given to a radio station to use a radio frequency or radio frequency channel under specified conditions.                                                                                                                                                                                                                                                                                                                  |
| <b>frequency hopping</b>    | The repeated switching of frequencies during radio transmission according to a specified algorithm, intended to minimize unauthorized interception or jamming of telecommunications.                                                                                                                                                                                                                                                         |
| <b>frequency modulation</b> | Modulation technique in which signals of different frequencies represent different data values.                                                                                                                                                                                                                                                                                                                                              |
| <b>frequency sharing</b>    | The assignment to or use of the same radio frequency by two or more stations that are separated geographically or that use the frequency at different times.                                                                                                                                                                                                                                                                                 |
| <b>function tone</b>        | A tone that follows the high level guard tone and causes the radio to perform a specific function, such as selecting a new transmit frequency. Function tones are often referred to as F1, F2, F3, and so on. <i>See</i> preamble and high level guard tone.                                                                                                                                                                                 |



---

## G

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>gateway</b>    | Device that performs an application-layer conversion of information from one protocol stack to another. In Cisco IPICS, the gateway component includes LMR gateways, which functionality is usually installed as an additional feature in a supported Cisco router. LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio frequencies to IP multicast streams.                                                                                 |
| <b>GRE</b>        | generic routing encapsulation. Tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment. GRE is generally used to route multicast traffic between routers. |
| <b>guard tone</b> | The most common guard tones are the high level guard tone (HLGT) and the low level guard tone (LLGT). The HLGT is used to alert the radio that a function tone follows. The LLGT is used as a hold tone or keying tone. <i>See</i> tone keyed.                                                                                                                                                                                                                                              |

---

## H

|                            |                                                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>H.323</b>               | Defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods to allow dissimilar communication devices to communicate with each other by using a standardized communication protocol. |
| <b>high-band frequency</b> | Refers to the higher frequency levels in the VHF band, typically 138-222 MHz.                                                                                                                                                    |

|                                      |                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HLGT</b>                          | high level guard done. Also known as awake tone. This tone is set at high volume and is usually the first tone in a preamble. It is used to alert the radio that another tone, usually a function tone, will follow. <i>See</i> guard tone.                                                                                                                |
| <b>Hoot 'n' Holler (Hootie)</b>      | <p>A communications system where the loudest and most recent talker or talkers are mixed into one multicast output stream. Also known as hootie, these networks provide “always on” multiuser conferences without requiring that users dial in to a conference.</p> <p>Cisco enables the Cisco Hoot 'n' Holler feature in specific Cisco IOS versions.</p> |
| <hr/>                                |                                                                                                                                                                                                                                                                                                                                                            |
| <b>idle tone</b>                     | The tone that a radio may deliver on the m-lead to signal the LMR gateway that there is no incoming traffic. When the idle tone is removed, the LMR gateway deems all signals to be valid voice traffic.                                                                                                                                                   |
| <b>inactive VTG</b>                  | A VTG that is stored for use. The Cisco IPICS server stores inactive VTGs with the information that you enter so that they can be automatically activated by a policy or manually activated by a dispatcher.                                                                                                                                               |
| <b>inband</b>                        | Traffic that is sent inband is included in the same stream as the real-time traffic protocol (RTP). Inband signals can be encoded signals and RFC 2833 signals.                                                                                                                                                                                            |
| <b>incident management framework</b> | A software framework that includes an adaptable GUI to facilitate resources, such as users, radio channels, cameras, and sensor information, for delivery that is based upon policy or incident needs.                                                                                                                                                     |
| <b>informix linux group</b>          | Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Informix database application. Members of this group include the informix and ipicsdba users.                                                                                                                                         |

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>informix user ID</b>   | <p>The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, this user has full administrative permission to the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.</p> <p>To access the informix user, log in to the Cisco IPICS server by using the root user ID; then, enter <b>su - informix</b> (superuser from root).</p> |
| <b>interference</b>       | <p>The effect of unwanted energy due to one or a combination of emissions, radiation, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information, which could be extracted in the absence of such unwanted energy.</p>                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>interoperability</b>   | <p>The capability of equipment manufactured by different vendors to communicate with each other successfully over a network.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>invitation policy</b>  | <p>A policy that can be invoked only through the telephony user interface and can include only the invite to VTG action. After joining a talk group, a user can access the breakout menu and invoke invitation policies. The talk group that this user has joined is the talk group that the invited users join.</p>                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>invite to VTG</b>      | <p>A version of the dial out invite action where users to be invited are preconfigured but the VTG that they are invited to depends on which VTG the invoker of the policy is dialed into.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>ipicsadmin user ID</b> | <p>The Cisco IPICS Linux user that, as part of the ipics linux group, has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. In addition, the ipicsadmin user has permission to read and write data from and/or to the Informix database. Cisco IPICS creates this Linux system user ID during the software installation process. The password for this user ID never expires.</p>                                                                                                                                                                                                                         |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipicsdba user ID</b>  | <p>The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, the ipicsdba user has permission to read data, write data, create tables, and create databases in the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.</p> <p>To access the ipicsdba user, log in to the Cisco IPICS server by using the root user ID; then, enter <b>su - ipicsdba</b> (superuser from root).</p> |
| <b>ipics linux group</b> | <p>Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. Members of this group include the ipicsadmin, ipicsdba, and informix users.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>ipics user ID</b>     | <p>The Cisco IPICS application-level user ID that can perform all administration-related tasks via the Cisco IPICS Administration Console. Cisco IPICS creates this web-based user ID during the software installation process.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>IPSec</b>             | <p>IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.</p>                                                                                                                                                                                                                                  |

---

## K

|                  |                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>keepalive</b> | <p>A message that is sent by one network device to inform another network device that the virtual circuit between the two devices is still active.</p> |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|

**key** The parameter that defines an encryption code or method.

Key (a radio) causes the radio to transmit. *See* tone keyed.

**kilohertz (kHz)** A unit of frequency that denotes one thousand Hz.

---

## L

**latch** The PMC functionality that allows a Cisco IPICS user to lock in a PTT channel.

**linear modulation** A radio frequency transmission technique that provides the physical transport layer of a radio system. This technology is compatible in digital and analog system environments and supports channel bandwidths of 5 kHz to 50 kHz.

**LLGT** low level guard tone. This tone is used as a hold tone or keying tone. *See* guard tone.

**LMR** Land Mobile Radio. A Land Mobile Radio (LMR) system is a collection of portable and stationary radio units that are designed to communicate with each other over predefined frequencies. They are deployed wherever organizations need to have instant communication between geographically dispersed and mobile personnel.

This term is often used interchangeably between a handheld or vehicle-mounted device and a stationary transmitter. Stationary devices are typically referred to as base stations.

Cisco IPICS leverages the Cisco Hoot 'n' Holler feature, which is enabled in specific Cisco IOS versions, to provide radio integration into the Cisco IPICS solution. LMR is integrated by providing an ear and mouth (E&M) interface to a radio or other PTT devices, such as Nextel phones. Configured as a voice port, this interface provides the appropriate electrical interface to the radio. You configure this voice port with a connection trunk entry that corresponds to a voip dial peer, which in turn associates the connection to a multicast address. This configuration allows you to configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

|                           |                                                                                                                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LMR gateway</b>        | Land Mobile Radio gateway. Refers to the router E&M interface that converts IP traffic from digital to analog for use by radios.                                                                                                                                                |
| <b>location</b>           | In Cisco IPICS, location signifies reachability; meaning, channels or users who are associated with the same location can communicate with each other without additional network configuration. Location may refer to a physical or virtual location, as defined in the server. |
| <b>low-band frequency</b> | Lower frequency levels in the VHF band, typically 25–50 MHz.                                                                                                                                                                                                                    |

---

## M

|                               |                                                                                                                                                                                                                  |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>megahertz (MHz)</b>        | A unit of frequency denoting one million Hz.                                                                                                                                                                     |
| <b>mixed tone</b>             | Two tones that are mixed together. DTMF is an example of a mixed tone. To be transmitted properly, tone signals must be mixed with the LLGT. <i>See</i> DTMF.                                                    |
| <b>m-lead</b>                 | The mouth portion of the E&M interface. The m-lead is the transmit path of the LMR gateway.                                                                                                                      |
| <b>modulation</b>             | The process, or result of the process, of varying a characteristic of a carrier in accordance with an information-bearing signal.                                                                                |
| <b>multicast</b>              | Single packets that are copied by the network and sent to a specific subset of network addresses. Multicast refers to communications that are sent between a single sender and multiple recipients on a network. |
| <b>multicast address</b>      | A single address that may refer to multiple network devices.                                                                                                                                                     |
| <b>multicast address/port</b> | Cisco IPICS uses this type of connection to enable the PMC to directly tune in to the multicast channel. Multicast address/port combinations are also used by gateways and RMS components.                       |
| <b>multicast pool</b>         | Multicast IP addresses that are defined as part of a multicast pool. Cisco IPICS allocates a multicast address from this pool of resources when a dispatcher activates a VTG.                                    |

|                            |                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>multiplexing</b>        | The combination of two or more information channels on to a common transmission medium. In electrical communications, the two basic forms of multiplexing are time-division multiplexing (TDM) and frequency-division multiplexing (FDM). |
| <b>multipurpose policy</b> | A policy that can include any of the supported actions; may be invoked through the telephony user interface or the Cisco IPICS administration console.                                                                                    |
| <b>multiselect buttons</b> | Provides the ability to select or deselect all channels on the PMC for audio transmission.                                                                                                                                                |
| <b>mute</b>                | The functionality that enables a dispatcher to mute a PMC user from talking or transmitting voice on one or more channels. The dispatcher can mute the microphone of the user or both the microphone and the speaker.                     |
| <b>mutual aid channel</b>  | A national or regional channel that has been set aside for use only in mutual aid interoperability situations. Restrictions and guidelines governing usage usually apply.                                                                 |

---

## N

|                                                                  |                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>narrowband channels</b>                                       | Channels that occupy less than 20 kHz.                                                                                                                                                                                                                                                                                                                |
| <b>National Public Safety Planning Advisory Committee</b>        | The committee that was established to conduct nationwide planning and allocation for the 821–824 MHz and 866–869 MHz bands.                                                                                                                                                                                                                           |
| <b>National Telecommunication and Information Administration</b> | The United States executive branch agency that serves as the principal advisor to the president on telecommunications and information policies and that is responsible for managing the federal government’s use of the radio spectrum.                                                                                                               |
| <b>near end</b>                                                  | The device or devices that are physically connected to the Ethernet or an RS-232 link. Compare with far end, which refers to devices on the other side of the broadcast. A base station that is connected to an LMR gateway is a near end device while a handheld radio that receives over-the-air signals from the base station is a far end device. |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>network</b>       | An interconnection of communications entities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>NAT</b>           | Network Address Translation. Provides a mechanism for translating addresses that are not globally unique into globally routable addresses for connection to the Internet.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>not activated</b> | A VTG state that becomes effective when the Activate button is clicked a second time (to deactivate the channel) or if the connection terminates. No PMC buttons appear highlighted.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>notification</b>  | <p>An action that notifies selected user(s) via email, SMS, pager, or phone. The necessary IDs and phone numbers are configured in the communication preferences for each user. Notifications that are sent via the phone require user authentication before the notification prompt is heard.</p> <p>An email, SMS, pager, or phone call that is placed to a user for the purpose of sending a notification message.</p>                                                                                                                               |
| <hr/> <b>O</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>offline mode</b>  | When the connection to the server goes offline, the PMC enters offline mode. Offline mode enables continuous communication during periods of server downtime. Using offline mode requires at least one successful login to the server.                                                                                                                                                                                                                                                                                                                  |
| <b>operator</b>      | The Cisco IPICS operator is responsible for setting up and managing users, configuring access privileges, and assigning user roles and ops views.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>ops view</b>      | operational view. A Cisco IPICS feature that provides the ability to organize users, user groups, channels, channel groups, VTGs, and policies into different user-definable views across multiple organizations or agencies that normally would not share resources. While ops views are maintained separately by the Cisco IPICS system administrator and/or ops view administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need. |



**ops view administrator**

The ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console (**Administration > Activity Log Management**) window.

**OTAR**

over-the-air re-keying. Provides the ability to update or modify over radio frequency the encryption keys that are programmed in a mobile or portable radio.

---

**P****packet**

A logical grouping of information that includes a header that contains control information. Usually also includes user data.

**packet switching**

The process of routing and transferring data by using addressed packets so that a channel is occupied during the transmission of the packet only. Upon completion of the transmission, the channel is made available for the transfer of other traffic.

**PIM**

Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: PIM dense mode and PIM sparse mode.

**PIM dense mode**

One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces until pruning and truncation occurs. In dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and will probably use the datagrams that are forwarded to them. The cost of using dense mode is its default flooding behavior. Sometimes called dense mode PIM or PIM DM.

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PIM sparse mode</b>         | One of the two PIM operational modes. PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. Sometimes called sparse mode PIM or PIM SM. |
| <b>PMC</b>                     | Push-to-Talk Management Center. A standalone PC-based software application that simulates a handheld radio to enable PTT functionality for PC users. This application enables Cisco IPICS PMC end-users, dispatch personnel, and administrators to participate in one or more channels/VTGs at the same time.                                                                                                                                                                                                                                                                      |
| <b>PMC ID</b>                  | The unique ID that the Cisco IPICS server generates for each PMC to track requests between the PMC and the server and to verify and manage concurrent PMC usage for licensing requirements.                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>policy</b>                  | Policies include one or more actions that execute sequentially and can be manually activated via the Cisco IPICS administration console or the telephony user interface. Cisco IPICS provides support for multiple policy types.                                                                                                                                                                                                                                                                                                                                                   |
| <b>policy channel</b>          | A channel that can be set up by the dispatcher and configured as a designated channel; that is, a channel that is always open to enable your interaction with the dispatcher.                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>policy execution status</b> | An indicator of policy execution success or failure. The Cisco IPICS administration console provides a status for each action under a policy.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>portalization</b>           | A web programming paradigm for customizing the interface and functionality of a client application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>preamble</b>                | The sequence of tones that precede a transmission. The preamble generally includes the HLGT and the function tone.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>protocol</b>                | A set of unique rules that specify a sequence of actions that are necessary to perform a communications function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|                           |                                                                                                                                                                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PTT</b>                | Push-to-talk. A signal to a radio transmitter that causes the transmission of radio frequency energy.<br><br>The action that keys a radio or causes the radio to transmit. On the Cisco router, the e-lead, or key tone, is used to signal the radio to transmit. |
| <b>PTT channel</b>        | A channel consists of a single unidirectional or bidirectional path for sending and/or receiving signals. In the Cisco IPICS solution, a channel represents one LMR gateway port that maps to a conventional radio physical radio frequency (RF) channel.         |
| <b>PTT channel button</b> | The button on the PMC that you click with your mouse, or push, and hold to talk. You can use the latch functionality on this button to talk on one or more channels at the same time.                                                                             |
| <b>PTT channel group</b>  | A logical grouping of available PTT channels that can be used for categorization.                                                                                                                                                                                 |

---

## Q

|                      |                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>QoS</b>           | quality of service. A measurement of performance for a transmission system, including transmission quality and service availability.                                                                       |
| <b>queue</b>         | Represents a set of items that are arranged in sequence. Queues are used to store events occurring at random times and to service them according to a prescribed discipline that may be fixed or adaptive. |
| <b>queuing delay</b> | In a radio communication system, the queuing delay specifies the time between the completion of signaling by the call originator and the arrival of a permission to transmit to the call originator.       |

---

## R

|                      |                                                                                                                                                                                    |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radio channel</b> | Represents an assigned band of frequencies sufficient for radio communication. The bandwidth of a radio channel depends upon the type of transmission and its frequency tolerance. |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radio control service</b> | The logical element in the Cisco IPICS system that can tune a radio to the desired channel without manual intervention. Refers to a serial control entity.                                                                                                                                                                                                                                                                                                                                               |
| <b>radio equipment</b>       | Any equipment or interconnected system or subsystem of equipment (both transmission and reception) that is used to communicate over a distance by modulating and radiating electromagnetic waves in space without artificial guide. This equipment does not include microwave, satellite, or cellular telephone equipment.                                                                                                                                                                               |
| <b>receive indicator</b>     | The indicator on the PMC that blinks green when traffic is being received.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>remote connection</b>     | Cisco IPICS uses this type of connection to provide SIP-based trunking into the RMS component, which is directly tuned into the multicast channel.                                                                                                                                                                                                                                                                                                                                                       |
| <b>RF</b>                    | radio frequency. Any frequency within the electromagnetic spectrum that is normally associated with radio wave propagation. RF generally refers to wireless communications with frequencies below 300 GHz.                                                                                                                                                                                                                                                                                               |
| <b>RFC 2833</b>              | The Internet Engineering Task Force (IETF) specification that describes how to carry DTMF signaling, other tone signals, and telephony events in RTP packets. Using RFC 2833 a packet can be compactly composed to play a series of tones, including DTMF, in a specific sequence that includes specified durations and volume levels.                                                                                                                                                                   |
| <b>RF repeater</b>           | An analog device that amplifies an input signal regardless of its nature (analog or digital). Also, a digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.                                                                                                                                                                                                                                                |
| <b>RMS</b>                   | <p>router media service. Component that enables the Cisco IPICS PMC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality.</p> <p>The RMS mixes multicast channels in support of VTGs and it also mixes PMC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.</p> |

|                     |                                                                                                                                                                                                                                                     |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>root user ID</b> | The Cisco IPICS Linux user that has access to all files in the Cisco IPICS server. Strong passwords are enforced and Linux operating system password expiration rules apply to this user ID.                                                        |
| <b>RTP</b>          | Real-Time Transport Protocol. Commonly used with IP networks to provide end-to-end network transport functions for applications that transmit real-time data, such as audio, video, or simulation data, over multicast or unicast network services. |
| <b>RTCP</b>         | Real-time Transport Control Protocol. The standard for notifying senders and receivers of important events or transmission statistics. The most common forms of RTCP are the sender report and the receiver report.                                 |

---

## S

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>scanning</b>                | A subscriber unit feature that automatically allows a radio to change channels or talk groups to enable a user to listen to conversations that are occurring on different channels or talk groups.                                                                                                                                                                                                                                                                                                                                                              |
| <b>script prompts</b>          | The audio prompts that the dial engine scripts play out during execution and which callers hear when they are interacting with the telephony user interface.                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>secure channel</b>          | <p>A channel that is connected to a radio that provides secure (encrypted or scrambled) communications on the Common Air Interface (CAI) side of the radio. (The level of security that is configured in the data network determines the security of the communications between the LMR gateway and a network attached device, such as a PMC or Cisco Unified IP Phone.)</p> <p>An attribute that is set in the server to indicate that a channel is secure. A PTT channel that is configured as secure cannot be combined with unsecure channels in a VTG.</p> |
| <b>serial controlled radio</b> | A type of control for a radio that uses out-of-band signaling (usually RS-232). <i>See</i> radio control service.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>service delivery area</b>   | <i>See</i> coverage.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>signal</b>                  | The detectable transmitted energy that carries information from a transmitter to a receiver.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                           |                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>skin</b>                               | Skins form the appearance of the PMC. In Cisco IPICS, skins are customizable and available in various options, including 4-channel and 8-channel mouse and touch screen formats.                                                                                                                                                                                    |
| <b>speaker arbitration</b>                | The procedure that is used to determine the active audio stream in a Push-to-Talk system.                                                                                                                                                                                                                                                                           |
| <b>spectrum</b>                           | <p>The usable radio frequencies in the electromagnetic distribution. The following frequencies have been allocated to the public safety community:</p> <p>High HF 25–29.99 MHz<br/>Low VHF 30–50 MHz<br/>High VHF 150–174 MHz<br/>Low UHF 406.1–420/450–470 MHz<br/>UHF TV Sharing 470–512 MHz<br/>700 MHz 764–776/794–806 MHz<br/>800 MHz 806–824/851–869 MHz.</p> |
| <b>spoken names</b>                       | The recorded names that are used for entities, such as channels, channel groups, VTGs, users, user groups, ops views, and policies. The names can be recorded through the policy engine or externally-recorded .wav files that can be uploaded into the system.                                                                                                     |
| <b>squelch</b>                            | An electric circuit that stops input to a radio receiver when the signal being received is too weak to be anything but noise.                                                                                                                                                                                                                                       |
| <b>statically configured tone control</b> | Every stream of data that flows to the LMR gateway can be applied with a preamble and/or guard tone by using a static configuration in the LMR gateway. When traffic is sent on a multicast address, the radio automatically switches (because of the preamble) to the specific radio channel that is requested by the tone control sequence.                       |
| <b>stored VTG</b>                         | Also referred to as inactive VTG.                                                                                                                                                                                                                                                                                                                                   |
| <b>subchannel</b>                         | A channel that shares the same multicast address as another channel or channels. These multiple source streams (channels) may be present on a single radio channel. On the PMC, you access these channels by pressing the channel selector buttons on the radio channel.                                                                                            |
| <b>subscriber unit</b>                    | A mobile or portable radio unit that is used in a radio system.                                                                                                                                                                                                                                                                                                     |

|                             |                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>system administrator</b> | The Cisco IPICS system administrator is responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. The system administrator also creates ops views, manages the Cisco IPICS licenses and PMC versions, and monitors the status of the system and its users via the activity log files. |
| <b>system architecture</b>  | The design principles, physical structure, and functional organization of a land mobile radio system. Architectures may include single site, multi-site, simulcast, multicast, or voting receiver systems.                                                                                                                                                               |
| <hr/>                       |                                                                                                                                                                                                                                                                                                                                                                          |
| <b>T</b>                    |                                                                                                                                                                                                                                                                                                                                                                          |
| <b>T1</b>                   | Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using alternate mark inversion (AMI) or binary 8 zero suppression (B8ZS) coding.                                                                                                                                                                   |
| <b>T1 loopback</b>          | Allows mapping from multicast to unicast so that unicast phone calls can be patched into an LMR or into other multicast audio streams. A loopback is composed of two of the available T1 interfaces.                                                                                                                                                                     |
| <b>talk group</b>           | <p>A VTG or a channel.</p> <p>A subgroup of radio users who share a common functional responsibility and, under normal circumstances, only coordinate actions among themselves and do not require radio interface with other subgroups.</p>                                                                                                                              |
| <b>TCP</b>                  | Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.                                                                                                                                                                                            |
| <b>TDMA</b>                 | time division multiple access. Type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval (“slot” or “slice”) for the transmission of each channel; that is, the channels take turns to use the link.                                                                                     |
| <b>terminal</b>             | A device capable of sending, receiving, or sending and receiving information over a communications channel.                                                                                                                                                                                                                                                              |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>throughput</b>            | The number of bits, characters, or blocks passing through a data communications system, or a portion of that system.                                                                                                                                                                                                                                                                                                                                                  |
| <b>TIA/EIA-102 standards</b> | A joint effort between government and industry to develop voice and data technical standards for the next generation of public safety radios.                                                                                                                                                                                                                                                                                                                         |
| <b>tone control</b>          | The process of using inband tone sequences to change the behavior of a radio end point. An inband tone can be used to control functions, such as modifying (retuning) the radio frequency (RF channel), changing the transmit power level, and monitoring a channel. The most basic form of tone control (tone keyed) is used to key the radio. With the Cisco IPICS solution, the radio that is being controlled is directly connected to the LMR gateway E&M leads. |
| <b>tone frequency</b>        | A specific form of a function tone. The tone that is used to signal the radio to select a frequency. These audible tone frequencies are generated in the router and combined in a specific sequence to perform a tone control function.                                                                                                                                                                                                                               |
| <b>tone keyed</b>            | A tone keyed radio requires the presence of a specific tone on the incoming analog (e-lead) port. Without this tone, the radio cannot transmit. The tone is generally used to prevent spurious transmission that may occur because of injected noise.                                                                                                                                                                                                                 |
| <b>tone signaling</b>        | Any form of over-the-air audible signals that are intended to terminate at the far end. Examples include alerting tones, DTMF tones, and paging tones.                                                                                                                                                                                                                                                                                                                |
| <b>transmit indicator</b>    | On some of the PMC skins, this indicator blinks red when traffic is being transmitted.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>trigger</b>               | A time-based event that invokes a policy on a scheduled basis, without manual intervention.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>trunk</b>                 | A physical and logical connection between two switches across which network traffic travels. In telephony, a trunk is a phone line between two central offices (COs) or between a CO and a PBX.                                                                                                                                                                                                                                                                       |
| <b>trunked (system)</b>      | Systems with full feature sets in which all aspects of radio operation, including RF channel selection and access, are centrally managed.                                                                                                                                                                                                                                                                                                                             |



|                             |                                                                                                                                                                                                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trunked radio system</b> | Integrates multiple channel pairs into a single system. When a user wants to transmit a message, the trunked system automatically selects a currently unused channel pair and assigns it to the user, decreasing the probability of having to wait for a free channel. |
| <b>TUI</b>                  | telephony user interface. The telephony interface that the dial engine provides to enable callers to perform tasks, such as joining talk groups and invoking policies.                                                                                                 |
| <b>tune (a radio)</b>       | To change the current send and receive frequencies on a radio. This task is usually accomplished via a preset with some form of radio control.                                                                                                                         |

---

## U

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>user</b>    | The Cisco IPICS user may set up personal login information, download the PMC application, customize the PMC skin, and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using the PMC, supported models of Cisco Unified IP Phones, and the Public Switched Telephone Network (PSTN) via the telephony dial functionality of the Cisco IPICS IP policy engine. Users may have one or more Cisco IPICS roles, such as system administrator, ops view administrator, operator or dispatcher. |
| <b>unicast</b> | Specifies point-to-point transmission, or a message sent to a single network destination.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

---

## V

|                        |                                                                                                                                                                                                                                                                                   |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VAD</b>             | Voice Activity Detection. When VAD is enabled on a voice port or on a dial peer, only audible speech is transmitted over the network. When VAD is enabled on Cisco IPICS, the PMC only sends voice traffic when it detects your voice.                                            |
| <b>virtual channel</b> | A virtual channel is similar to a channel but a radio system may not be attached. By creating a virtual channel, participants who do not use physical handheld radios to call into a VTG become enabled by using the PMC application or a supported Cisco Unified IP Phone model. |

|                               |                                                                                                                                                                                                                                                                 |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>voice interoperability</b> | Voice interoperability enables disparate equipment and networks to successfully communicate with each other.                                                                                                                                                    |
| <b>voice replay</b>           | A feature that allows the PMC user to replay buffered audio on a per channel basis.                                                                                                                                                                             |
| <b>VoIP</b>                   | Voice over Internet Protocol. By digitalizing and packetizing voice streams, VoIP provides the capability to carry voice calls over an IP network with POTS-like functionality, reliability, and voice quality.                                                 |
| <b>volume indicator</b>       | The volume indicator on the PMC that shows the current volume level on the channel in a graphical format.                                                                                                                                                       |
| <b>volume up/down buttons</b> | The buttons on the PMC that let you control the volume level.                                                                                                                                                                                                   |
| <b>VOX</b>                    | Voice-operated transmit. A keying relay that is actuated by sound or voice energy above a certain threshold and sensed by a connected acousto-electric transducer. VOX uses voice energy to key a transmitter, eliminating the need for push-to-talk operation. |
| <b>VTG</b>                    | virtual talk group. A VTG can contain any combination of channels, channel groups, users, and user groups. A VTG can also contain other VTGs.                                                                                                                   |
| <b>VTG add participant</b>    | An action that adds selected participant(s) to the selected VTG.                                                                                                                                                                                                |

---

## W

|                         |                                                                    |
|-------------------------|--------------------------------------------------------------------|
| <b>wavelength</b>       | The representation of a signal as a plot of amplitude versus time. |
| <b>wideband channel</b> | Channels that occupy more than 20 kHz.                             |



## INDEX

---

### Numerics

404 or 500 error after logging in to Administration Console [3-10](#)

---

### A

#### Administration Console

- browser guidelines [3-3](#)
- cannot log in [3-4](#)
- cannot log in with ipics user ID [3-24](#)
- cannot perform tasks [3-14](#)
- changes not saved when multiple users are configuring [3-22](#)
- not functioning [3-14](#)

---

### B

#### browser

- refreshing window [3-16](#)
- troubleshooting access to the server [3-4](#)

browser guidelines [3-3](#)

---

### C

cablelength router command [4-10](#)

#### CallManager

*See* Cisco Unified CallManager

#### CallManager Express

*See* Cisco Unified CallManager Express

call waiting, dial-in calls disconnect after using [3-38](#)

cannot deactivate

stopping state, in RMS [4-16](#)

cannot log in to administration console [3-24](#)

catalina.out log file [7-1](#)

caution, described [xvii](#)

#### caveats

application troubleshooting [5-29](#)

CLI commands [5-12](#)

troubleshooting [5-29](#)

VPN client [5-17](#)

changing IP address, troubleshooting problems [3-32](#)

changing server IP address [6-4](#)

changing system date and time, problems with time-bound licenses [3-32](#)

#### channel

- choosing codec [4-8, 4-9](#)
- feedback noise [4-6](#)
- PMC deactivates by itself [4-5](#)
- troubleshooting access to multiple channels [4-2](#)
- troubleshooting multicast address problems [4-2](#)
- channels
  - connectivity failure indicator [5-26](#)
  - visual indicators
    - connectivity failure [5-26](#)
- characters, language, incorrect display [3-20](#)
- checking status of the license manager [2-9](#)
- Cisco IOS
  - documentation [xvi](#)
- Cisco IPICS Activity Log [7-2](#)
- Cisco IPICS IP Policy Engine
  - See* policy engine
- Cisco IPICS operating system
  - See* operating system, Cisco IPICS
- Cisco IP Phone
  - See* Cisco Unified IP Phone
- Cisco IP Phones
  - documentation [xv](#)
- Cisco Land Mobile Radio (LMR)
  - documentation [xvi](#)
- CisconnnMIVRnnnn.log file [7-2, 7-3](#)
- Cisco Security Agent
  - documentation [xvi](#)
- Cisco Security Agent (CSA)
  - checking status [6-9](#)
  - documentation [7-17](#)
  - logs [7-7, 7-15](#)
  - security event log, opening [7-16](#)
  - starting [2-18, 6-9](#)
  - starting, stopping, and restarting [6-9](#)
  - stopping [2-18, 6-9](#)
- Cisco Unified Communications Manager (CallManager)
  - documentation [xiv](#)
- Cisco Unified Communications Manager Express
  - documentation [xv](#)
- Cisco Unified IP Phone
  - cannot access channel [4-13](#)
  - cannot communicate with PMCs in a channel [4-12](#)
  - no power [4-11](#)
  - one-way audio after receiving or placing a phone call [4-12](#)
  - radio users cannot hear IP phone users [4-6](#)
  - troubleshooting power problems [4-11](#)
  - voice quality issues with policy engine dial-in or dial-out calls [4-9](#)
- Cisco Unified IP phone
  - 404 or host not found message [4-13](#)
  - cannot access Cisco IPICS service
    - Cisco IPICS service, cannot use after changing server IP address [4-13](#)
  - clear counters router command [4-10](#)
  - clear line router command [4-18](#)

clock source router command [4-10](#)

codec, voice quality and [4-8, 4-9](#)

command, server

enableuser [3-26, 6-3](#)

modify\_ip [6-4](#)

ntpsetup [6-5](#)

reset\_pw [3-24, 6-7](#)

service ciscosec [6-9](#)

service iippe\_dial\_engine [6-10](#)

service ipics [6-9](#)

service ipics\_db [6-9](#)

service ipics\_lm [3-29, 6-9](#)

service ipics\_tomcat [6-10](#)

Command failed error [3-20](#)

communication issue

PMCs and Cisco Unified IP Phones cannot communicate on a channel [4-12](#)

some PMCs cannot talk on channel [4-3](#)

VTG participants cannot hear each other [4-2, 4-3](#)

communication issues, VTGs and SIP PMCs [4-9](#)

connectivity, verifying with ping command [3-7](#)

connectivity indicators

SIP-based remote connections [5-26](#)

controller, limiting number of DS0s [4-16](#)

conventions, document [xvi](#)

csalog log file [7-2](#)

## D

database server

checking status [2-7, 6-9](#)

manually starting [3-7](#)

performing procedures [2-6](#)

restarting [2-8](#)

starting [2-9, 6-9](#)

stopping [2-8](#)

troubleshooting [3-14](#)

db-maintenance.log file, about [7-3, 7-4](#)

deactivating RMS, to edit router details [4-19](#)

deactivation fails for RMS [4-16](#)

debugging

PMC [7-10](#)

using CLI-based tools and service commands [6-1](#)

using log files [7-1](#)

diagnostics.log file [7-4](#)

dial engine

checking status [2-13, 6-10](#)

error after uploading prompt file [3-35](#)

PARTIAL\_SERVICE status [3-46](#)

performing service procedures [2-12](#)

restarting [2-14](#)

starting [2-15](#)

starting and stopping [6-10](#)

stopping [2-14](#)

voice quality problems [4-9](#)

dial engine, starting and stopping [6-10](#)

## dial-in calls

disconnect after using hold or call waiting feature [3-38](#)

do not connect [3-39](#)

radio users cannot hear dial-in users [4-6](#)

dial-out calls, radio users cannot hear dial-out users [4-6](#)

dial-out invites do not connect [3-43](#)

dial-out notifications do not connect [3-44](#), [3-46](#)

disabled user, enabling with enableuser command [6-3](#)

## documentation

Cisco IOS [xvi](#)

Cisco IP Phones [xv](#)

Cisco Land Mobile Radio (LMR) [xvi](#)

Cisco Security Agent [xvi](#), [7-17](#)

Cisco Unified Communications Manager (CallManager) [xiv](#)

Cisco Unified Communications Manager Express [xv](#)

conventions [xvi](#)

MCS servers [xv](#)

double-byte language support [5-27](#)

driverManager.log files [7-4](#)

DS0, limiting number on router [4-16](#)

DSCP [4-8](#)

DSPs, insufficient [4-3](#)

---

**E**

echoes, in conferences [4-22](#)

e-mail, outgoing notifications do not connect [3-44](#), [3-46](#)

enableuser command [6-3](#)

enabling a disabled user with enableuser command [6-3](#)

encrypted file system [5-5](#)

## error

404 or 500, in browser [3-10](#)

authorization after changing ipics user password [3-24](#)

command failed [3-20](#)

PMC gets unknown response [3-21](#)

undefined javascript [3-19](#)

error messages [5-30](#)

---

**F**

## feedback

in conferences [4-22](#)

on VTG or channel [4-6](#)

finding troubleshooting information [1-1](#)

## footswitch

troubleshooting [5-7](#)

---

**G**

G.711 codec, voice quality and [4-8](#)

G.729 codec, voice quality and [4-8](#)

G711 codec, voice quality and [4-9](#)

G729 codec, voice quality and [4-9](#)

---

## H

hardware, locating MAC address for [3-28](#)

headset

- resolving headset issues [5-11](#)

hold, dial-in calls disconnect after using [3-38](#)

host mismatch error, troubleshooting [3-28, 3-32](#)

---

## I

IE publisher error [5-15](#)

ifconfig command, using to obtain MAC address [3-28](#)

information

- finding Cisco IPICS troubleshooting [1-1](#)

informix user, resetting password [3-14, 6-7](#)

install.log file [7-4](#)

installation, troubleshooting [3-1](#)

installation log file [5-3](#)

Internet Explorer

- browser error [3-10](#)
- refreshing browser window [3-16](#)
- troubleshooting browser access to the server [3-4](#)

Internet Explorer browser guidelines [3-3](#)

invitations, dial-out invites do not connect [3-43](#)

IP address

- changing [6-2](#)
- troubleshooting problems after changing [3-32](#)

verifying Cisco IPICS [3-7](#)

ipics.log file [7-5](#)

ipics\_audit.log file [7-5](#)

ipics\_pmc.log file [7-6](#)

ipics\_rms.log file [7-6](#)

ipicsadmin user, resetting password [3-24, 6-7](#)

ipics-install-log.txt log file [7-5](#)

ipics user, resetting password [6-7](#)

IP Phone

- See* Cisco Unified IP Phone

---

## J

javascript error, troubleshooting undefined [3-19](#)

---

## L

language characters, incorrect display [3-20](#)

license

- all features do not display after loading multiple license files [3-31](#)
- locating MAC address [3-28](#)
- troubleshooting after changing IP address [3-32](#)
- troubleshooting installation [3-27, 3-32](#)
- troubleshooting time-bound [3-32](#)
- troubleshooting time-bound license files [3-32](#)

license manager

checking status [2-9, 2-10, 6-9](#)

restarting [2-11, 6-9](#)

starting [2-12, 6-9](#)

stopping [6-9](#)

lmgrd.log file [7-6](#)

location

incorrectly configured [4-13](#)

locked user, unlocking with enableuser command [6-3](#)

log files

catalina.out [7-1](#)

Cisco IPICS Activity Log [7-2](#)

CisconnnMIVRnnnn.log [7-2, 7-3](#)

Cisco Security Agent (CSA) [7-15](#)

csalog [7-2](#)

db-maintenance [7-3, 7-4](#)

diagnostics.log [7-4](#)

driverManager.log [7-4](#)

install.log [7-4](#)

ipics.log [7-5](#)

ipics\_audit.log [7-5](#)

ipics\_pmc.log [7-6](#)

ipics\_rms.log [7-6](#)

ipics-install-log.txt [7-5](#)

lmgrd.log [7-6](#)

PMC, modifying levels [7-7](#)

securitylog.txt [7-7](#)

tacout [7-7](#)

login, cannot log in after changing password [3-24](#)

loopback, indicator lights for [4-21](#)

low level guard tone (LLGT), E&M port does not transmit after a port deactivation and activation [4-6](#)

---

## M

MAC address, obtaining [3-28](#)

MCS servers

documentation [xv](#)

Media category, PMC DebugLog.txt [7-10, 7-14](#)

Microsoft QoS Packet Scheduler [4-8](#)

modify\_ip command [6-4](#)

multicast

troubleshooting problems [4-2](#)

---

## N

network processes, starting and stopping with CLI commands [6-9](#)

Network Time Protocol (NTP)

logs [7-7](#)

Network Time Protocol (NTP), configuring [6-5](#)

no prompt router command [4-18](#)

note, described [xvii](#)

notifications, dial-out notifications do not connect [3-44, 3-46](#)

ntpsetup command [6-5](#)



## O

### one-way audio

between PMC and Cisco Unified IP Phone [4-12](#)

with Cisco Unified IP Phone after placing or receiving a phone call

troubleshooting

one-way audio problems with  
Cisco Unified IP  
phones [4-12](#)

one-way audio issues [5-11](#)

### operating system, Cisco IPICS

checking database status [2-7](#)

checking tomcat service status [2-2](#)

database procedures [2-6](#)

database server procedures [2-6](#)

restarting database [2-8](#)

starting database [2-9](#)

starting tomcat service [2-5, 2-6](#)

stopping

tomcat service [2-3](#)

tomcat service procedures [2-2](#)

ops views, dial-out notifications do not work  
between ops views [3-46](#)

## P

packets, IP marked incorrectly [4-8](#)

Packet Scheduler, Microsoft QoS [4-8](#)

PARTIAL\_SERVICE status

for dial engine [3-46](#)

for subsystem manager [3-46](#)

### password

changing, for root user [3-25, 6-7](#)

resetting

for informix user [3-24, 6-7](#)

for ipicsadmin user [3-24, 6-7](#)

for ipics user [3-24, 6-7](#)

PIM, sparse and sparse-dense modes [4-2](#)

ping command, using to verify Cisco IPICS IP  
address [3-7](#)

pins, mapping for a T1 on router [4-22](#)

### PMC

cannot communicate with IP Phones in a  
channel [4-12](#)

caveats

application troubleshooting [5-29](#)

CLI commands [5-12](#)

VPN client [5-17](#)

deactivates channel by itself [4-5](#)

log entries [7-6](#)

poor voice quality [4-8](#)

SIP-connected voice communication  
interrupted [4-9](#)

some cannot communicate on channel [4-3](#)

troubleshooting

application [5-1](#)

audio and headset issues [5-11](#)

audio settings [5-7](#)

caveats [5-29](#)

- channel activation issues [5-26](#)
- Cisco Security Agent [5-9](#)
- codec misconfiguration [5-27](#)
- coexistence [5-10](#)
- configuration file changes [5-6](#)
- connectivity issues [5-16](#)
- DNS issues [5-25](#)
- error messages [5-30](#)
- execution [5-2](#)
- footswitch device [5-7](#)
- generating a PMC installation log file [5-3](#)
- headset [5-8](#)
- headset issues [5-12](#)
- high latency, low bandwidth links [5-25](#)
- microphone [5-9](#)
- multicast connections [5-21](#)
- offline mode [5-23](#)
- one-way audio [5-11](#)
- one-way audio issues [5-13](#)
- optional settings menu [5-6](#)
- publisher error [5-15](#)
- QoS Packet Scheduler [5-20](#)
- resolving IP address changes [5-13](#)
- right-to-left and double-byte language support [5-27](#)
- RMS connectivity [5-24](#)
- satellite connectivity [5-25](#)
- server administration GUI access issues [5-15](#)
- unknown response error [3-21](#)
- using an encrypted file system [5-5](#)
- voice quality [5-14](#)
- VPN issues [5-16](#)
- VTG not appearing on [3-17](#)
- Windows XP firewall [5-19](#)
- winsock corruption [5-22](#)
- users are not logged out after terminating session [4-4](#)
- using debugging log level [7-10](#)
- voice quality degrades for SIP user [4-8](#)
- PMC DebugLog.txt [7-9, 7-12](#)
- PMC log levels, modifying [7-7](#)
- PoE module [4-11](#)
- policy, VTG not activating in [3-16](#)
- policy engine
  - cannot communicate with the prompt manager [3-38](#)
  - checking dial engine status [2-13](#)
  - log files [7-2](#)
  - performing dial engine service procedures [2-12](#)
  - restarting dial engine [2-14](#)
  - starting and stopping [6-9](#)
  - starting the dial engine [2-15](#)
  - stopping dial engine [2-14](#)
  - voice quality problems from dial engine [4-9](#)
- processes, Cisco IPICS, starting and stopping [6-9](#)
- prompt file, error after uploading [3-35](#)

prompt manager error messages [3-38](#)

## Q

QoS, Microsoft Packet Scheduler [4-8](#)

## R

radio

- low level guard tone not sent after E&M port deactivation and activation [4-6](#)

- users in channel cannot hear Cisco Unified IP Phone or policy engine users [4-6](#)

recovering a deleted user with system administrator privileges [3-23](#)

refreshing browser window [3-16](#)

reset\_pw command [6-7](#)

resetting passwords, for ipics, ipicsadmin, informix and root users [6-7](#)

restarting

- database [2-8, 6-9](#)

- dial engine [2-14](#)

- license manager [2-11, 6-9](#)

- tomcat service [6-10](#)

restore, PMC gets error after [3-21](#)

right-to-left language support [5-27](#)

RMS [4-16](#)

- configuration, long wait after restarting Cisco IPICS [4-16](#)

- deactivating [4-19](#)

- failing [4-18](#)

limiting DS0s on router [4-16](#)

log entries [7-6](#)

no loopbacks displayed on new [4-19](#)

PMC connectivity to the RMS [5-11](#)

SIP-based connectivity [5-26](#)

troubleshooting connectivity issues [5-24](#)

unrecognized T1 ports [4-20](#)

updating login information causes unreachable state [4-19](#)

root user

- resetting password [6-7](#)

router

- clear line command [4-18](#)

- configuration shows wrong information [4-22](#)

- insufficient DSPs on [4-3](#)

- IOS software version [4-11](#)

- long delays between pressing PMC PTT button and media establishment [4-24](#)

- long wait for restart after configuring [4-16](#)

- mapping pins for T1 [4-22](#)

- no green indicator lights [4-21](#)

- no loopbacks displayed on new RMS [4-19](#)

- no prompt command [4-18](#)

- PIM modes [4-2](#)

- PoE module [4-11](#)

- show users command [4-18](#)

- slow VTG activation [4-18](#)

- T1 configuration [4-10](#)

- unreachable state [4-18, 4-19](#)

updating configuration in Cisco  
IPICS [4-22](#)

VTY lines [4-18](#)

router media service

*See* RMS

## S

security events log, Cisco Security Agent,  
opening [7-16](#)

securitylog.txt file [7-7](#)

server, database

checking status [2-7](#)

manually starting [3-7](#)

restarting [2-8](#)

starting [2-9](#)

stopping [2-8](#)

server administration GUI access issues [5-15](#)

service ciscosec command [6-9](#)

service ipics\_db command [6-9](#)

service ipics\_lm command [3-29, 6-9](#)

service ipics\_tomcat command [6-10](#)

service ipics command [6-9](#)

service ippe\_dial\_engine command [6-10](#)

Show Configuration feature [4-22](#)

show users router command [4-18](#)

SHUTDOWN status, for SIP subsystem [3-47](#)

Signaling category, PMC DebugLog.txt [7-10, 7-13](#)

SIP-based connection

connection failure [5-26](#)

SIP subsystem

SHUTDOWN status [3-47](#)

spoken name prompt file, error after  
uploading [3-35](#)

starting

dial engine [2-15](#)

starting Cisco Security Agent [2-18](#)

starting database server [2-9](#)

starting the license manager [2-12](#)

starting tomcat service [2-5, 2-6](#)

status

checking database server [2-7, 6-9](#)

checking dial engine [6-10](#)

checking license manager [6-9](#)

checking policy engine [6-9](#)

checking tomcat service [2-2, 6-10](#)

stopping

Cisco Security Agent [2-18, 6-9](#)

database server [2-8, 6-9](#)

dial engine [2-14, 6-10](#)

license manager [6-9](#)

policy engine [6-9](#)

tomcat service [6-10](#)

stopping tomcat service [2-3](#)

subsystem manager, PARTIAL\_SERVICE  
status [3-46](#)

system administrator user, recovering a deleted  
user [3-23](#)

- ## T
- T1
    - configuration [4-10](#)
    - loopbacks not displayed on new RMS [4-19](#)
    - mapping pins on router [4-22](#)
    - unrecognized ports [4-20](#)
  - TAC Case Collection Tool [5-15](#)
  - tacout log file [7-7](#)
  - time-bound license
    - troubleshooting [3-32](#)
  - tomcat service
    - checking status [2-2, 3-4, 6-9, 6-10](#)
    - performing procedures [2-2](#)
    - restarting [3-5, 3-22](#)
    - starting [2-5, 2-6, 6-9, 6-10](#)
    - stopping [2-3, 6-9, 6-10](#)
  - troubleshooting
    - 404 or 500 error in browser
      - 404 error [3-10](#)
    - Administration Console not functioning [3-14](#)
    - authorization error after changing password [3-24](#)
    - cannot reach server from browser [3-4](#)
    - Cisco Unified IP Phone cannot access channel [4-13](#)
    - Command failed error [3-20](#)
    - communication disrupted [4-9](#)
    - configuration changes not saved when multiple users are configuring [3-22](#)
    - connectivity between Cisco Unified Wireless IP Phone 7920 models [4-14](#)
    - database stopped [3-14](#)
    - dial engine [3-46](#)
    - dial engine voice quality [4-9](#)
    - dial-in call cannot reconnect after using call waiting feature [3-38](#)
    - dial-in call disconnects after placing on hold [3-38](#)
    - dial-in calls [3-39](#)
    - dial-out invites [3-43](#)
    - dial-out notifications [3-44, 3-46](#)
    - displaying loopbacks in Add Router window [4-19](#)
    - feedback noise on VTG, channel [4-6](#)
    - host mismatch error [3-28, 3-32](#)
    - installation issues [3-1](#)
    - language characters display incorrectly [3-20](#)
    - license installation [3-27, 3-32](#)
    - login problems from browser [3-4](#)
    - multicast problems [4-2](#)
    - new RMS has no loopbacks [4-19](#)
    - no green lights on router [4-21](#)
    - non-activating policy [3-16](#)
    - no power to Cisco Unified IP Phones [4-11](#)
    - no table data [3-19](#)
    - password problems, ipicsadmin or informix user [3-24](#)
    - password problems for ipics user [3-24](#)
    - password problems for root user [3-25](#)

PMC deactivates channel by itself [4-5](#)  
 PMCs cannot communicate on channel [4-3](#)  
 PMC users not logged out after terminating session [4-4](#)  
 policy engine voice quality [4-9](#)  
 poor PMC voice quality [4-8](#)  
 poor voice quality for SIP-based PMC [4-8](#)  
 power for Cisco Unified IP Phones [4-11](#)  
 RMS fails [4-18](#)  
 router configuration long delays between pressing PMC PTT button and media establishment [4-24](#)  
 router configuration shows wrong information [4-22](#)  
 SIP subsystem [3-47](#)  
 slow VTG activation [4-18](#)  
 subsystem manager [3-46](#)  
 time-bound licenses [3-32](#)  
 tomcat service not running [3-4](#)  
 undefined javascript error [3-19](#)  
 unreachable RMS state after updating login [4-19](#)  
 unreachable router state [4-18](#)  
 unresponsive Cisco IP Phone channel [4-13](#)  
 unresponsive PMC channel [4-3](#)  
 using CLI-based tools and service commands [6-1](#)  
 using log files [7-1](#)  
 voice loops in conferences [4-22](#)  
 VTG activating itself [3-15](#)  
 VTG feedback [4-6](#)

VTG not appearing on PMC [3-17](#)

VTG participants cannot communicate [4-2](#), [4-3](#)

troubleshooting the PMC application [5-1](#)

---

## U

unlocking a locked user [6-3](#)

unreachable state on router [4-18](#), [4-19](#)

Update Configuration feature [4-22](#)

user ID, multiple IDs for same user [3-17](#)

user interface, PMC debug log information [7-9](#), [7-12](#)

---

## V

voice, poor quality from policy engine dial-in or dial-out calls [4-9](#)

voice, poor quality on PMC [4-8](#)

voice, poor quality with dial engine calls [4-9](#)

voice loops [4-22](#)

voice quality

issues [5-14](#)

VTG

activates by itself [3-15](#)

feedback noise [4-6](#)

not activating in policy [3-16](#)

not appearing on PMC [3-17](#)

participants cannot hear each other [4-2](#), [4-3](#)

slow activation [4-18](#)

voice interruptions [4-9](#)  
VTY lines [4-18](#)

