Cisco IP Interoperability and Collaboration System (IPICS) Troubleshooting Guide

Release 1.0(1)

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

Customer Order Number:
Text Part Number: OL-8362-01

Cisco IPICS Troubleshooting Guide

Preface

The *Cisco IP Interoperability and Collaboration System (IPICS) Troubleshooting Guide* provides you with the information that you need to troubleshoot problems you may encounter when you install, configure, or use the Cisco IPICS 1.0(1) software. System administrators should review this document to aid their troubleshooting efforts for problems that they may encounter on the Cisco IPICS Administration Console, the Cisco IPICS PMC application, and other Cisco IPICS components.

Hardware and Software Compatibility

For a list of hardware and software requirements for Cisco IPICS, refer to the *Cisco IPICS Server Installation Guide*.

For a current list of compatible versions for all Cisco IPICS components, see the Cisco IPICS Compatibility Matrix document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Where to Find Troubleshooting Information

The Cisco IPICS Administration Console informs you of most errors with messages that display at the top of the current window. Cisco IPICS error messages clearly indicate any incorrect user actions and how to recover from them.

If errors occur in the software or in a Cisco IPICS component such as an RMS, most of these errors are written to the ipics.log file. You can view the latest entries in the ipics.log file in the System Status window of the Administration Console. For information about the System Status window, see the "The System Status Window" section on page 1.

Some errors that can occur in Cisco IPICS are not written to the ipics.log file and may appear in one of several other logs on the Cisco IPICS server. For information on these logs, see the "Viewing Cisco IPICS Logs" section on page 11.

For a listing of the information that is available for problems that you might encounter in Cisco IPICS, see Table 1.

Table 1 Locating Troubleshooting Information

Source of Problem	Where to Find Help
Issues with one of the following areas: • Cisco IPICS installation • Communication between Cisco IPICS users • Equipment, such as Cisco IP Phones • Router configuration • General operation	Many common issues that can occur in these areas are described in Chapter 5, "Troubleshooting the Cisco IPICS Server." The descriptions include information on how to resolve the issues or where to look for additional information. If you need more information to resolve the issue, you can gather data from one of the Cisco IPICS logs. For log information, see the "Downloading System Logs" section on page 6 or "Viewing Cisco IPICS Logs" section on page 11
PMC Issues	Problems that you may encounter when installing or using the PMC application are described in Chapter 6, "Troubleshooting the PMC Application." If you need more information to resolve the issue, you can gather data from one of the PMC logs. For log information, see the "Modifying the PMC Log Levels" section on page 1
Backup and Restore Issues	You can obtain information about backing up or restoring the Cisco IPICS database or about any problems that you encounter in the backup or restore process in the *Cisco IPICS Backup and Restore Guide*.

For information on other documentation resources, see the "Related Documentation" section on page xii and the "Accessing Additional Information" section on page xiii

Audience

The *Cisco IPICS Troubleshooting Guide* targets end users 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 a PMC or Cisco IP Phone.

Organization

This document is organized as follows:

Chapter 1, "Managing Cisco IPICS Processes"	This chapter includes procedures that are related to Cisco IPICS server processes, such as the Tomcat service and the Informix database.
Chapter 2, "Understanding the Cisco IPICS Logs"	This chapter includes information about the activity and error logs and the configuration files that Cisco IPICS uses or maintains.
Chapter 3, "Monitoring the Cisco IPICS System Status"	This chapter includes information about monitoring the database status, purge activity logs, and view and download system logs.
Chapter 4, "Managing Cisco IPICS Options"	This chapter includes information about setting system preferences in the Options window of the Administration Console.

Chapter 5, "Troubleshooting the Cisco IPICS Server"	This chapter includes information about troubleshooting issues that may arise in the installation of the Cisco Linux operating system and Cisco IPICS server software, the setup and configuration of the Cisco IPICS server, or the use of the Administration Console.
Chapter 6, "Troubleshooting the PMC Application"	This chapter includes information about troubleshooting issues that may arise in the setup, configuration, or use of the PMC Application.
Appendix A, "Changing the Cisco Linux Root Password"	This appendix includes instructions for changing the Cisco Linux root password after the Cisco IPICS server software has been installed.

Related Documentation

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

- *Cisco IPICS Server Administration Guide, Release 1.0(1)*—This document contains information about the key configuration, operation, and management tasks for the Cisco IPICS server.
- *Cisco IPIS Server Installation Guide, Release 1.0(1)*—This document describes how to install and configure the Cisco IPICS 1.0 server software and Cisco Linux operating system.
- *Cisco IPICS PMC Installation and User Guide, Release 1.0(1)*—This document describes how to install, configure, manage, and operate the Cisco IPICS PMC application

- *Cisco IPICS PMC Quick Start Guide, Release 1.0(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 Guide, Release 1.0(1)*—This document provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC.
- *Cisco IPICS Backup and Restore Guide, Release 1.0(1)*—This document describes the administrative procedures that you use to backup and restore the database files on the Cisco IPICS server.
- *Cisco IPICS Command Line Interface, Release 1.0(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.
- *Release Notes for Cisco IPICS Release 1.0(1)*—This document contains a description of the new and changed features, important notes, caveats, and documentation updates for Cisco IPICS release 1.0(1).
- *Cisco IPICS Compatibility Matrix*—This document contains information about compatible hardware and software that is supported for use with Cisco IPICS.
- *Cisco IPICS 1.0(1) Resources Card (Documentation Locator)*—This document includes a summary of the documentation that is available for Cisco IPICS release 1.0(1).

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

http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Accessing Additional Information

Cisco IPICS Information

See the Cisco IPICS documentation for detailed information and procedures for the Cisco IPICS Administration Console and the PMC application. For a full list of Cisco IPICS documents, see the "Related Documentation" section on page xii.

Voice Troubleshooting

For information about voice quality problems and symptoms, see 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

IP Multicast Troubleshooting Information

For a description of common problems and solutions that relate to using IP multicast, see the following link and search for the *IP Multicast Troubleshooting Guide.* You can also use this link to search for general IP multicast information:

http://www.cisco.com/warp/public/732/Tech/multicast/

Cisco CallManager Documentation

For information about Cisco CallManager, see the documentation at this URL:

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

Cisco 7800 Series Media Convergence Servers Documentation

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

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

Cisco IP Phone Documentation

For information about Cisco IP Phones, see the documentation at this URL:

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

Cisco Land Mobile Radio over IP

For information about Cisco Land Mobile Radio (LMR) over IP, see the documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/lmrip/index.htm

Cisco Security Agent

For information about Cisco Security Agent (CSA), see the documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/

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, see the documentation at this URL:

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

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 document.

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 2 Conventions

Convention	Description
boldface font	Commands and keywords appear in **boldface**.
italic font	Command input for which you supply the values appear in *italics.*
[ ]	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 *Control*. For example, when you read ^*D* or *Ctrl-D*, 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.
italic screen font	Arguments for which you supply values are in *italic screen* font.

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Cisco will continue to support documentation orders using the Ordering tool:

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

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

- Instructions for ordering documentation using the Ordering tool are at this URL:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

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

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

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

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and

Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

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

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

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

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

Managing Cisco IPICS Processes

When you start the Cisco IPICS server, the server software automatically starts the following components:

- Tomcat service
- Informix database
- Cisco Security Agent

There may be circumstances in which you need to manually stop or start one of these components. To do so, you must log in to the Cisco IPICS server and perform command line interface (CLI) procedures in a Cisco Linux terminal window.

This chapter also includes the procedure that you need to follow to change the root user password on the Cisco IPICS server.

Tip This chapter describes how to perform procedures directly on the Cisco IPICS server by using a terminal window from the Cisco Linux desktop. You can also perform these procedures by connecting to the Cisco IPICS server remotely by using the SSH Tectia Client.

This chapter includes the following sections:

Performing Tomcat Service Procedures

The Tomcat service is the main Cisco IPICS process and contains all of the Cisco IPICS web applications. For the Cisco IPICS server software to function, the Tomcat service must run continuously.

Cisco IPICS provides a cron job that checks the status of the Tomcat service every 60 seconds and can restart the service automatically, if the Tomcat service stops. The automatic restart occurs based on a setting in the tomcatcron file, which is located in the **/opt/cisco/ipics/tomcat** directory.

When the RESTART_TOMCAT_ON_ERROR value in the tomcatcron file is set to true, the cron job attempts to restart the Tomcat service if the service stops. If this value is set to false, the cron job continues to check the Tomcat service status, but does not attempt to restart the service.

If the cron job makes an attempt to restart the service, the CRON_ERROR_COUNT value in the tomcatcron file changes from 0 to 1. If the restart attempt is unsuccessful, the cron job continues to attempt the restart until the CRON_ERROR_COUNT reaches 3.

After the third attempt, the cron job continues to monitor the Tomcat service status, but does not make further attempts to restart the service. If you start the Tomcat service manually, the cron job will recognize that the Tomcat service has started again and will reset the CRON_ERROR_COUNT to 0.

If you need to perform a maintenance function that requires stopping the Tomcat service, you must adjust the RESTART_TOMCAT_ON_ERROR value. To stop the Tomcat service and adjust the file, see the "Stopping the Tomcat Service" section on page 1-3

This section includes the following topics related to the Tomcat service:

Checking the Status of the Tomcat Service

If the Tomcat service stops and the cron job cannot restart it, none of the features in Cisco IPICS can operate. In this event, users would be unable reach the Cisco IPICS Administration Console.

If you cannot access Cisco IPICS with your browser, check the status of the Tomcat service by performing the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

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

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

```
root      5270     1  2 11:30 ?        00:01:33
/opt/cisco/ipics/jre/bin/java -server -Xms64m -Xmx256m -DMP_DATA=
-Djava.security.auth.login.config==/opt/cisco/ipics/tomcat/security/
.java.login.config
-Djava.security.auth.policy==/opt/cisco/ipics/tomcat/security/
.java.policy -Djava.util.logging.manager=org.apache.juli.
```

If the Tomcat service is not running, the response to the grep command is similar to the following example:

```
root      5773  5723  0 12:29 pts/1    00:00:00 grep tomcat
```

If the grep command shows that the Tomcat service is not running, you can start it manually by using a CLI procedure. For more information, see "Starting the Tomcat Service" section on page 1-5.

Stopping the Tomcat Service

If you perform a procedure such as database maintenance, you may have to stop the Tomcat service to avoid user logins. However, because of the cron job that restarts Tomcat automatically, you must first temporarily stop the cron job.

To stop the Tomcat service, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Stop the automated restart routine in the cron job by performing the following procedure:

a. To locate the tomcatcron file so that you can halt the automatic restart process, navigate to the /opt/cisco/ipics/tomcat directory by entering the following command:

[root] **#cd /opt/cisco/ipics/tomcat**

b. To edit the tomcatcron file, enter the following command:

[root] **#vi tomcatcron**

Cisco Linux opens the file for editing. The RESTART_TOMCAT_ON_ERROR setting specifies true (activated) by default.

c. To deactivate the restart routine, you must edit the RESTART_TOMCAT_ON_ERROR value and change the setting to false. You can adjust the setting by using the **Arrow** keys to move your cursor over the word, true. Then, press x to delete each letter.

d. To enter characters, press **I** to insert and then enter characters. Press **Esc** when you have finished entering characters.

e. When you have finished editing, enter **:wq!** and then press **Enter** to save the file.

Note Make sure that you repeat Steps a through e to set the RESTART_TOMCAT_ON_ERROR value to true again after you complete your maintenance and manually restart the Tomcat service.

Step 4 To stop the Tomcat service, enter the following command at the prompt:

[root] **#/etc/init.d/ipics_tomcat stop**

If the Tomcat service stops successfully, Cisco Linux displays the message, [OK].

If the Tomcat service does not successfully stop, Cisco Linux displays an error message. If you cannot stop the Tomcat service, continue to Step 5.

Step 5 If the Tomcat service fails to stop, you can kill the processes that are running by performing the following procedure:

a. To check what Tomcat processes are still running, enter the following command:

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

The grep command returns information about the Tomcat processes that are still running. Note the Process IDs, which display in the second column of the grep results.

b. To stop any Tomcat processes that are still running, enter the following command:

[root] **#kill -9 *<process ID>***

c. Repeat Step b for every Tomcat process that is running.

d. Delete the tomcat.pid file by entering the following command:

[root] **#rm -rf /var/run/tomcat.pid**

e. Remove the /var/lock/subsys/ipics_tomcat directory by entering the following command:

[root] **#rm -rf /var/lock/subsys/ipics_tomcat**

After completing this procedure, you can safely start the Tomcat service again. For more information, see the "Starting the Tomcat Service" section on page 1-5.

Starting the Tomcat Service

Cisco IPICS starts the Tomcat service as part of the initial start-up process. A cron job regularly checks the Tomcat service status and restarts the service if the Tomcat service stops.

However, if the cron job fails to start the Tomcat service successfully or if you stop the service, you can also start the Tomcat service manually.

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

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ipics_tomcat start**

If you successfully started the Tomcat service Cisco Linux displays the message, [OK].

Note There may be a delay of a few minutes before users can access the Administration Console after the Tomcat service starts.

Step 4 Edit the tomcatcron file to reactivate the automated restart routine by adjusting the RESTART_TOMCAT_ON_ERROR setting to true. To adjust this setting, use the procedure in Step 3 in the "Stopping the Tomcat Service" section on page 1-3.

If the Tomcat service does not successfully start, check the catalina.out file (or catalina.*x-x-x*.log, where *x-x-x* is the date on which the file was created), which is located in the following directory:

/opt/cisco/ipics/tomcat/versions/5.5.9/logs

If you cannot resolve the problem with the information in the log files, contact Cisco Support.

Restarting the Tomcat Service

If you need to restart the Tomcat service when it is already running, you can use the restart command, which stops the Tomcat service and then starts it again. This procedure is helpful for circumstances such as activating the ops view feature after uploading and applying the license.

When you restart the Tomcat service, users are automatically logged out of the Administration Console and must log back in again.

To restart the Tomcat service, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ipics_tomcat restart**

After stopping, and then again after starting, the Tomcat service, Cisco Linux displays the message, [OK].

Note There may be a delay of a few minutes before users can access the Administration Console after the Tomcat service restarts.

Performing Informix Database Procedures

In rare circumstances, you may need to stop or start the Informix database, which you can do by enter CLI commands in a Cisco Linux terminal window on the Cisco IPICS server. To check the status of the database, you can enter a CLI command or open the System Status window in the Administration Console.

This section includes the following topics:

Checking the status of the Informix Database

Cisco IPICS includes the Administration Console GUI that allows the system administrator to check the status of the Informix database. See the "The System Status Window" section on page 3-1 for more information.

However, if you cannot log in to the Cisco IPICS Administration Console through the Login window with a valid user ID and password, you can manually check the status of the Informix database.

To check the database status from a Cisco Linux terminal window, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#ps -ef | grep oninit**

If the database is running properly, the grep command returns a process similar to the following example:

```
informix  5575     1  0 Oct26 ?        00:00:50
/opt/cisco/ipics/database/current/bin/oninit -r
root      5576  5575  0 Oct26 ?        00:00:08
/opt/cisco/ipics/database/current/bin/oninit -r
root      5577  5576  0 Oct26 ?        00:00:02
/opt/cisco/ipics/database/current/bin/oninit -r
root      5578  5576  0 Oct26 ?        00:00:00
/opt/cisco/ipics/database/current/bin/oninit -r
```

```
root      5579  5576  0 Oct26 ?        00:00:01
/opt/cisco/ipics/database/current/bin/oninit -r
root      5580  5576  0 Oct26 ?        00:00:00
/opt/cisco/ipics/database/current/bin/oninit -r
root     15750 15700  0 14:12 pts/1    00:00:00 grep oninit
```

If the database is not running, the response to the grep command is similar to the following example:

```
root     15750 15700  0 14:12 pts/1    00:00:00 grep oninit
```

If the grep command indicates that the database is not running, start the database. For more information, see the "Starting the Informix Database" section on page 1-10l.

Stopping the Informix Database

Stopping the Informix database would only be necessary if you discover that the database is slowing the performance of Cisco IPICS.

Note If you are experiencing slow performance for Cisco IPICS activity, you could determine whether the database is causing this effect only by checking the amount of system resources that the database is consuming. To perform this check, use the Cisco Linux **top** command from a Cisco Linux terminal window or an SSH Tectia Client window.

To stop the Informix database, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ipics_db stop**

If the database stops successfully, Cisco Linux displays the message, [OK].

If the database does not successfully stop, Cisco Linux displays an error message. If you cannot stop the database, continue to Step 4.

Step 4 If the database fails to stop, you can kill the processes that are running by performing the following procedure:

a. To check what database processes are still running, enter the following command:

[root] **#ps -ef | grep oninit**

The grep command returns information about the database process that are still running. Note the Process IDs, which display in the second column of the grep results.

b. To stop any database processes that are still running, enter the following command:

[root] **#kill -9 *<process ID>***

c. Repeat Step b for every database process that is running.

Starting the Informix Database

Cisco IPICS starts the Informix database as part of the initial start-up process. You can also start the Informix database manually, if you determine that the database has stopped for any reason. To check whether the database is running, see the "Checking the status of the Informix Database" section on page 1-8.

To manually start the Informix database from a Cisco Linux terminal window, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ipics_db start**

If you successfully started the database, Cisco Linux displays the message, [OK].

If the database does not successfully start, check the diagnostics.log file, which is located in the following directory:

/opt/cisco/ipics/database/logs

If you cannot resolve the problem with the information in the log file, contact Cisco Support.

Performing Cisco Security Agent Procedures

Cisco Security Agent (CSA) prevents the user (or an intruder) from performing actions on the Cisco IPICS server that may disable the server. There may be times where stopping CSA is necessary to perform system-level functions, to debug an issue, or to edit system files.

Note If you chose not to install CSA when you installed the Cisco IPICS server software, you can install CSA at any time by using a CLI procedure in a Cisco Linux terminal window.

If you installed CSA, there may be situations where you need to manually uninstall the software. For information about manually installing or uninstalling CSA, refer to the *Cisco IPICS Server Installation Guide*.

This section includes the following topics:

Viewing CSA 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 access these messages in the following ways:

The CSA utility Messages pane

To view status messages in the CSA utility Messages pane, double-click the CSA tray icon (the red flag) to open the utility. The Messages pane displays by default.

Security Event Log in the CSA utility

To view the Security Event Log in the CSA utility, double-click the CSA tray icon (the red flag) to open the utility. Then, click **View Logs**.

Security Event Log in a text view

To view the Security Event Log in a text viewer, perform the following procedure:

Step 1 To view the contents of the log directory, open a terminal window by clicking the **Red Hat** icon. Then, choose **System Tools > Terminal**.

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 in the directory, enter the following command:

[root] **#ls -l**

The contents of the directory display. The Security Event Log file is named csalog. If the file has reached the maximum size one or more times, there will be more than one csalog file in the directory. Subsequent files are named csalog.0, csalog.1, csalog.2, and so on. The log that has the largest numeric extension is the current file.

Step 4 To view the log file, enter the following command:

[root] **#cat csalog.*x***

where *x* is the numeric extension, if applicable.

A text viewer window displays the contents of the Security Event Log.

Stopping CSA

You can temporarily stop CSA with the Cisco Security Agent utility or by issuing a command in a Cisco Linux terminal window.

This section includes the following topics:

Stopping CSA with the CSA Utility

To stop the CSA process in the CSA utility, perform the following procedure:

Procedure

Step 1 To stop CSA, open the CSA utility by performing one of the following actions:

- Click the **Red Hat** icon from the Cisco Linux desktop and choose **Cisco Security Agent > Cisco Security Agent**
- Click the CSA tray icon (the red flag)

Step 2 To display the current security setting, click **System Security**.

Step 3 To stop CSA, drag the Security Level button to **Off**.

Step 4 Click **OK**.

Level 0 indicates that CSA is turned off. The CSA utility window closes.

Stopping the CSA Using a CLI Procedure

To stop the CSA from a Cisco Linux terminal window, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ciscosec stop**

If you successfully stop CSA, Cisco Linux displays the message, [OK].

Starting CSA

If you installed it 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 it in the CSA utility or by performing a CLI procedure from a Cisco Linux terminal window.

This section includes the following topics:

Starting the CSA with the CSA Utility

To start the CSA process in the Cisco Security Agent utility, perform the following procedure:

Procedure

Step 1 To start the Cisco Security Agent utility program, perform one of the following actions:

- Click the **Red Hat** icon from the Cisco Linux desktop and choose **Cisco Security Agent > Cisco Security Agent**.
- Double-click the CSA tray icon (the red flag) to open the utility.

The Cisco Security Agent utility displays.

Step 2 To display the current security setting, click **System Security**.

Step 3 To start the Cisco Security Agent, drag the Security Level button to **Medium**.

Step 4 Click **OK**.

The security level changes to Medium and the CSA utility window closes.

Starting CSA Using a CLI Procedure

To start the CSA process from a Cisco Linux terminal window, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ciscosec start**

If you successfully start CSA, Cisco Linux displays the message, [OK].

Changing the Cisco Linux Root Password

You can change the password for the Cisco Linux root user on a periodic basis to ensure system security. You should also change the password immediately if you suspect that it is known to an unauthorized person.

To change the Cisco Linux root user password, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 To temporarily disable the Cisco Linux restrictions that apply to changing the root password, enter the following command:

[root] **#sh /root/.security/unimmunize.sh**

Step 4 To create a new root password, enter the following command:

[root] **#passwd**

Cisco Linux displays a message that it is changing the password for the root user.

Step 5 At the New Password prompt, enter a new root password and press **Enter**.

When you enter your password, no characters display.

Note Your new password must be a minimum of six characters and cannot be based on a dictionary word.

Step 6 At the Retype New Password prompt, enter the new password again and press **Enter**.

Step 7 If your password is valid and you retyped it correctly, the following message displays:

```
passwd: all authentication tokens updated successfully.
```

Step 8 To reenable the Cisco Linux restrictions that apply to changing the root password, enter the following command:

[root] **#sh /root/.security/immunize.sh**

Step 9 To close the terminal window, click **X**.

The Linux desktop displays.

Understanding the Cisco IPICS Logs

This chapter describes the information that you can obtain from the Cisco IPICS logs. The log information can aid you in troubleshooting problems that may occur with the Cisco IPICS and the PMC application.

This chapter includes the following sections:

Modifying the PMC Log Levels

The PMC application can generate logs that can be helpful when you analyze user activity and troubleshoot problems you may encounter when using 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. The logs are transferred to the server during its normal communication with the PMC.

This section has the following topics:

Users can generate PMC logs in the following ways:

- The PMC user can adjust settings within the PMC application. Refer to the *Cisco IPICS PMC Installation and User Guide* for more information.
- From the Administration Console, the Cisco IPICS operator can modify the log settings in the User Details area of the Manage Users window. See the "Setting PMC Log Levels in User Details" section on page 2-10 for more information.

The PMC can generate the following log files:

Table 2-1 PMC Log File Descriptions

PMC Log File Name	PMC Log File Description
Authentication.log	This log file contains a history of all user login and logout attempts per PMC installation. This log appears in XML format.
ChannelStatistics.log	At regular and predefined intervals, this log records each channel's statistics, including data for both sent and received transmissions over the network. This log appears in XML format.
UserInterface.log	This log contains a history of the user interactions with the PMC application. This log appears in XML format.
DebugLog.txt	This log contains debugging information that is relevant to how the PMC operates. You can track several different categories of debugging information and adjust the log levels to three different settings within each category. The DebugLog appears in text format and is rotated each time that the user starts the PMC application. For detailed information about the Debug Log, see the "Understanding Debug Log Information" section on page 2-3.

The default behavior for the DebugLog.txt file is to capture activity for the PMC, such as critical errors, IP changes, and so on. Initially, this log contains the PMC version and system statistics, such as the media devices that are installed on the system (headsets, microphones, and so on). The other PMC logs do not get produced until you set, except Channel Activation which is on by default.

Note You can obtain activity information for PMC users in the Activity Logs window of the Administration Console. This information includes details about user associations to channels and VTGs, channel activation activities, and conference participation. For information about using the Activity Logs window, refer to the *Cisco IPICS Server Administration Guide*.

Cisco IPICS retrieves logs from the PMC when one of the following events occur:

- You request a log in the User Details pane of the Administration Console Manage Users window.
- 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 only 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 the file to be uploaded.

After Cisco IPICS completes the upload, the PMC automatically deletes the file from the hard disk of the client machine.

Understanding 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 communications problems with the Cisco IPICS server.

  Table 2-2 describes the type of information you can gather with the User Interface log levels.

Table 2-2 User Interface Log Levels

Logging Level	Purpose
1	Useful for debugging the following types of issues: • The user is not able to log in • The user receives error messages from the server • The PMC goes into offline mode unexpectedly • The user has difficulty activating channels • The user has problems when closing the PMC application
2	This information can assist with translating server XML communications.
3	Issues 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 2-3 describes the type of information you can gather with the Signaling log levels.

Table 2-3 Signaling Log Levels

Logging Level	Purpose
1	Issues that involve the high level state machines.
2	Issues that involve the high level state machines.
3	Issues that involve 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 2-4 describes the type of information you can gather with the Media log levels.

Table 2-4 Media Log Levels

Logging Level	Purpose
1	This information provides RX and TX networking statistics.
2	This information can assist you to diagnose audio mixing issues, such as the combining of audio signals in a channel or VTG.
3	This information can assist in the area of converting 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 particular fields that you want to capture in the log.

Table 2-5 show the fields that are included in each logging level.

The log levels for each category are cumulative. If you choose Level 2 for a category, the PMC writes Level 1 and Level 2 fields into the DebugLog.txt file. When you set the logging to Level 3, you capture all the fields for that category.

Tip Always start debugging by collecting Level 1 data, which may provide all the data you require. Using Log Level 1 allows you to gather several days of log activity and not fill hard disk of the PMC user. If you cannot locate the cause of the problem, you can set the logging to Level 2 or Level 3.

Use Level 3 only for short durations. You can also closely monitor the hard drive of the user, so that the Level 3 logs do not overwhelm the client hard drive or strain 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 your debugging tasks have been completed, be sure to turn off debug logging by clearing the debug log.

Table 2-5 lists the fields that are associated with each DebugLog section:

Table 2-5 DebugLog Fields and Log Levels

Category	Field	Log Level
User Interface	channel-activation-debug	1
	error	
	exit-debug	
	sending-source-debug	
	sock-init-cleanup	
	xml-events	2
	xml-post	
	xml-vars	
	Auth	3
	critical-section-tune-debug	
	xml-deck	
	gui-debug	
	server-task-debug	
	server-verbose	

Table 2-5 DebugLog Fields and Log Levels (continued)

Category	Field	Log Level
Signaling	cc	1
	fim	
	fsm	
	gsm	
	lsm	
	multicast-signaling-debug	
	sip-reg-state	
	sip-state	
	vcm	
	sip-task	2
	sip-trx	
	Auth	3
	cc-msg	
	sip-messages	

Table 2-5 DebugLog Fields and Log Levels (continued)

Category	Field	Log Level
Media	AMuteTrans	1
	AudioSink	
	AudioSource	
	MediaStream	
	OpenALAudioSink	
	RTPAudioSink	
	RTPAudioSockets	
	RTPAudioSource	
	RTPAudioStream	
	RTPJitterBuf	
	sock-init-Cleanup	
	WaveAudioSource	
	WaveFileSource	
	RxStats	
	TxStats	

Table 2-5 DebugLog Fields and Log Levels (continued)

Category	Field	Log Level
Media	RxDetailStats	2
	ACMTrans	
	dsp	
	FilePlay	
	PCMMixer	
	PCMVolTrans	
	PCMVolumeMax	
	VAD	
	RTPAudioStreamMgr	
	AudioDump	3
	AudioSamp	
	AudioSampLost	
	AudioSampMgr	
	AudioTrans	
	dtmf	
	FIRTrans	
	FSAudioBuf	
	G7112PCMTrans	
	G7232PCMTrans	
	G729A2PCMTrans	
	Limiter	
	PCM2G711Trans	
	PCM2G723Trans	
	PCM2G729ATrans	
	TimeSample	

Setting PMC Log Levels in User Details

Note You must have operator privileges in Cisco IPICS to access the Manage Users window of the Administration Console.

In the User Details pane of the Manage Users window, you can instruct the Cisco IPICS server to retrieve updated activity logs for a particular PMC user. For the DebugLog.txt file, you can also set a logging level to retrieve specific types of debugging information.

After you obtain the logs that you need, you can easily reset or adjust your log settings by using the following procedure in this section. The log settings that you configured in the User Details pane remain will persist until you change them back to the default (or any other) settings.

Caution The User Details pane displays the new log settings for a user after you change them. Be sure to note the changes you make and the users for whom you made them, so that you can reset the log levels to the default setting after you finish your troubleshooting.

To define log settings and retrieve the file in the User Details pane, follow this procedure:

Procedure

Step 1 From the Operator tab in the Cisco IPICS Administration Console, click the **Manage Users** link.

Step 2 Click a user from the All Users list and then click **Details**.

Step 3 To set the log level for the desired log, use the drop-down lists under the Set PMC Log Level heading. You can set the log levels to the following settings:

- Authentication—Choose 1 to turn the logging on for this log; choose 0 to turn logging off
- User Interface—Choose 1 to turn the logging on for this log; choose 0 to turn logging off

- Channel Statistics—Choose 1 to turn the logging on for this log; choose 0 to turn logging off.
- Debug Log—Choose from one of the following log level options:
  - 1 to capture Level 1 fields
  - 2 to capture Level 1 and Level 2 fields
  - 3 to capture fields for all Log Levels

Step 4 To save the new log levels, click **Save**.

The log level settings display in the User Details pane and Cisco IPICS sends the new log level information to the PMC.

Step 5 Wait for the PMC to collect the log or debugging data.

If you have set the Debug Log to Level 3 in any category, monitor the disk space that the file consumes, so that it does not cause a problem for the user.

Step 6 To retrieve the file, click **Get** in the User Details pane.

Cisco IPICS sends a request (when the PMC next polls the server) to retrieve the specified log. Then, the PMC deletes the file from the hard disk of the PMC client machine.

You can find the retrieved logs in the directory for the PMC user. Cisco IPICS stores the log files in the following directory:

/opt/cisco/ipics/tomcat/current/webapps/ipics_server/pmclogs/<*user_ID*>

where *user_ID* is the user ID for the PMC that you are debugging.

Step 7 When you have completed the debugging for this PMC user, use the drop-down lists under Set PMC Log Levels to reset the log levels to 0 for all logs.

Step 8 Click **Save**.

Viewing Cisco IPICS Logs

Cisco IPICS generates several logs that can be useful in troubleshooting problems that you may encounter. The Cisco IPICS logs are located in the following directory:

/opt/cisco/ipics/tomcat/current/logs

Table 2-6 lists the Cisco IPICS logs that you can use for debugging.

Table 2-6 Cisco IPICS Logs

Log Name	Description
ipics.log	Cisco IPICS writes any known errors to the ipics.log file. When the log reaches approximately 5 MB in size, a new ipics.log is created and the previous logs are closed and archived. The most current entries in the ipics.log display in the System Status window of the Administration Console. For more information about the ipics.log file, see the "Downloading System Logs" section on page 3-6.
catalina.out	If non-typical errors occur in the Cisco IPICS server software or its components, the activity that caused the error may be captured in the catalina.out log.
ipics.rms.log	The ipics.rms.log collects log data for the RMS components that have been added to the Cisco IPICS database. When the log reaches approximately 1 MB in size, a new ipics.rms.log is created and the previous logs are closed and archived.
ipics_audit.log	The ipics_audit.log records, in XML format, every button that any Cisco IPICS user has clicked when using the Cisco IPICS system.
bar_act.log	This log captures information that relates to the Cisco IPICS backup and restore procedures. You can view the log in the Manage Database window of the Administration Console. For more information, refer to the *Cisco IPICS Backup and Restore Guide*.

Checking CSA Logs

If CSA denies a system action, the process generates a message that you can access in several ways. You can open the CSA Utility to view the messages in the Message pane or you can view the Security Events Log, which includes all security events that have occurred on the system.

You can view the latest Security Events Log in the CSA Utility or you can navigate to the /var/logs directory, where you can access the current and archived logs.

The file name of the Security Event Log is csalog. After seven days, CSA creates a new log and renames the previous log with a numbered extension. This process repeats every seven days, so that the logs are named csalog.0, csalog.1, csalog.2, and so on. The oldest log in the directory has the highest numbered extension.

This section includes the following topics:

Viewing the CSA Utility Messages Pane

To view status messages in the CSA utility, click the CSA tray icon (the red flag) to open the CSA Utility. Then, click **Messages**.

Status messages display in the Messages pane.

Opening the Security Events Log from the CSA Utility

To view the Security Events Log in the CSA Utility, perform the following procedure:

Step 1 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**.

Step 3 Click **View Log**.

The current Security Events Log displays in a text viewer window.

Opening a Security Events Log with a CLI Command

If you navigate to the **/var/log** directory, you can view the current log or any of the archived logs. You can view them by entering a CLI command.

To view a security event log with a CLI command, perform the following steps:

Step 1 Log in to the Cisco IPICS terminal with root, informix, or system user privileges.

The Cisco Linux desktop displays.

Step 2 To view the contents of the **/var/log** directory, open a Cisco Linux terminal window by clicking the **Red Hat** icon. Then, choose **System Tools > Terminal**.

A terminal window displays.

Step 3 To navigate to the /var/log directory, enter the following command:

Step 4 [root] **#cd /var/log**

Step 5 To view a list of the files in the directory, enter the following command:

Step 6 [root] **#ls -al**

The contents of the directory display. The security event logs are named csalog.*x*, where *x* is the numerical archive extension for the file. The most current log is named csalog and has no numerical extension.

Step 7 To view the contents of a log file, enter the following command:

Step 8 [root] **#cat csalog.*x***

For information about the messages that appear in the CSA logs, see the CSA documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/

Monitoring the Cisco IPICS System Status

Cisco IPICS provides the system administrator with the ability to view the status of the database and the latest database log information in the System Status window. The system administrator can download logs to view on screen or to save them to a file. If database files are no longer needed, the system administrator can purge them from the system.

This chapter includes the following sections:

The System Status Window

The System Status window displays the state of the Cisco IPICS database and the percentage of the database capacity that has been consumed by activity logs. If the activity log percentage rises to a critical level (85% or more of the stated capacity), you should purge some or all of the activity logs, according to the date range you specify. For information about purging activity logs, see the "Purging Activity Logs from the Database" section on page 3-4.

Note The percentage of database capacity shown in the System Status window is only current as of the time you opened or last refreshed the window. To see the new current percentage, you must click **Refresh Now** or activate the Auto Update feature. For more information, see the "Adjusting the Auto Update Setting" section on page 3-3.

The System Status window displays the content of the latest ipics.log file in the Recent System Log Entries pane. If any serious errors (any that are designated as ERROR or FATAL) occur, those log entries display in red in the pane. Use the scroll bar to view all the entries in Recent System Log Entries pane. For information about downloading the system logs, see the "Downloading System Logs" section on page 3-6.

Table 3-1 describes the types of system log entries that can appear in the Recent System Log Entries pane.

Table 3-1 System Log Entry Types

Log Entry Type	Purpose
TRACE	Fine-grained debug information (maximum detail) about the programmatic steps that Cisco IPICS performs to fulfill a request.
DEBUG	Debug information that is less detailed than TRACE information.
INFO	Informational message about noteworthy events, such as the starting of a scheduled policy.
WARN	Warning message about occurrences such as incorrect user input or requests that Cisco IPICS cannot fulfill.
ERROR	Message that is similar to a WARN message, but with higher severity, such as in the case of insufficient licenses. ERROR messages display in red in the Recent System Log Entries pane

Table 3-1 System Log Entry Types (continued)

Log Entry Type	Purpose
FATAL	When a FATAL error occurs, Cisco IPICS generates an error notification message and displays the message prominently in the current window of any user with system administrator or All privilege. Also, FATAL messages display in red in the Recent System Log Entries pane. A FATAL message concerns an unrecoverable error that requires your attention, such as a failed database connection or a router initialization failure. If you encounter a fatal error, see the [list of FATAL errors and how to troubleshoot].

Note By default the TRACE and DEBUG messages are not captured in the system logs. You would only activate these logging levels at the instruction of Cisco Support.

The System Status window displays by default when you log into the Administration Console or if you click the **System Administrator** tab from another user tab. To open the System Status window from another System Administrator window, click the **System Status** link.

Adjusting the Auto Update Setting

When you refresh the System Status window, Cisco IPICS refreshes the browser window and displays new information to the System Status indicators, such as the System Status field and the Database % Full field. The database status can be either Running or Offline. Refreshing the window also updates the Recent System Log Entries.

To monitor changes in these statuses, you can click **Refresh Now** at any time. You may also set the System Status window to refresh automatically at a specified interval by using the Auto Update setting.

Note The Auto Update setting is only active for the time that you are viewing the System Status window. When you close the browser or click another link in the Administration Console, the Auto Update feature resets to the None setting.

To modify the Auto Update setting, perform the following procedure:

Procedure

Step 1 In the System Status window of the Administration Console, choose the number of seconds for the interval between refreshes from the drop-down list box.

Step 2 Click **Apply**.

Cisco IPICS refreshes the window at the interval that you chose.

Step 3 To reset the Auto Update to the default setting (None), perform one of the following actions:

- Choose **None** from the drop-down list; then click **Apply**.
- Click another link or tab in the Administration Console.

  When you return to the System Status window, Cisco IPICS resets the Auto Update setting to None.

Purging Activity Logs from the Database

Cisco IPICS collects activity log information so that you can search for and view specific activities that are related to the users, PTT channels and VTGs in your Cisco IPICS system. For information about using the activity logs, refer to the *Cisco IPICS Server Administration Guide*.

Caution Make sure that you closely monitor the activity logs to minimize the database consumption. If the activity logs are not monitored, they can fill up the Cisco IPICS dbspace, which is the database partition that Cisco IPICS allots to all records. If your database becomes completely filled by the activity logs, your system may become inoperable.

To help safeguard against total database consumption, Cisco IPICS includes the Database % Full indicator. This indicator allows you to view the percentage of allotted disk space that has been consumed by the activity logs. To see the most current usage, click **Refresh Now**.

Caution The Database % Full indicator does not control the size of the activity logs; it provides an indication of when you should purge the activity logs.

When the consumption percentage for the activity logs reaches 85%, the color of the indicator turns from blue to red to indicate that you are approaching a database full level. You can choose to purge logs at any time, however.

Before you purge the activity logs, you can download them from the Activities Log window. To open the Activities Log window, click the **Download Activities Log** link in the Manage System area of the System Status window.

When you purge the logs, you can choose to purge just a portion of the logs, according to a date range. To purge activity logs from the database, perform the following procedure:

Procedure

Step 1 To choose a date range for the purge, choose a starting date and time by using the drop-down lists that displays next to the From field.

Tip To ensure that you purge the oldest activity logs in the database, set the year in the starting date to 2005.

Step 2 Choose an ending date and time by using the drop-down lists that displays next to the To field.

Step 3 Click **Purge**.

Cisco IPICS refreshes the System Status window. If you entered a valid date range for the activity logs in your database, the Database % Full indicator should display a lower percentage than it did before you performed the purge operation. If the indicator does not display a lower percentage, check that you entered a valid date range or try a larger range.

If your Database % Full indicator fills up quickly and causes you to purge your activity logs on a frequent basis, you can modify the Maximum Activity Logs setting in the Options window. For more information, see Chapter 4, "Managing Cisco IPICS Options."

Downloading System Logs

Cisco IPICS displays the most current system log information in the Recent System Log Entries pane and allows you to download all the system logs to your PC.

Cisco IPICS records system log information in the ipics.log file and continues to add data to it until the file reaches a size of approximately 5.2 MB. Then, Cisco IPICS renames the file with an incremental number (starting at 1) and creates a new ipics.log file to capture the most current log data. This process of filling and incrementing files continues until you have ten system log files that range from ipics.log.1 to ipics.log.10, plus the most recent ipics.log file. Cisco IPICS automatically purges the oldest file when you have accumulated ten files.

When you download your system logs, Cisco IPICS creates a zip file of all the ipics.log files.

The system logs are located in the following directory:

/opt/cisco/ipics/tomcat/current/logs

To download the system logs, perform the following procedure:

Procedure

Step 1 Below the Recent System Log Entries pane, click **Download**.

The Download dialog box displays.

Step 2 Take one of the following actions:

- To open the zip file, click **Open**.

  The zip file opens and displays the list of ipics.log files. If you wish, you can double-click one of the files to view it in WordPad or in another text file viewer on your PC.

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.

- To save the zip file to your PC, click **Save**.

  A Save As dialog displays, from which you can navigate to the location to save the zip file on your PC.

Step 3 If you chose to save the zip file, click **Save**.

Cisco IPICS saves the zipped log files to the specified location and closes the Save As window.

Managing Cisco IPICS Options

Cisco IPICS provides the system administrator with the ability to adjust system preferences and turn on or off certain options in the Options window. Cisco IPICS allows you to restore default settings at any time.

You can access the Options window from the Administration Console by navigating to **System Administrator > Options**.

Table 4-1 describes the settings that are available in the Options window. You can use the controls in the Options window in the following ways:

- To customize the settings in the Options window, edit the values according to the description in Table 4-1. Then, click **Save**.

  Note Ensure that you click **Save** after each change that you make to the settings.

- To discard changes that you make to the settings, click **Revert**.

  Note You must click **Revert** before you click **Save** or your changes do not revert to the previous settings.

- To restore all settings to the default values, click **Restore Defaults**.

Table 4-1 Option Window Settings and Controls

Setting	Description	Default Setting
Ops Views	When checked, this check box activates the Cisco IPICS ops views feature. For information about ops views, refer to the *Cisco IPICS Server Administration Guide*. **Note** If you enable the ops views feature, you must first restart the Tomcat service before you can use the feature. For information about stopping and starting the Tomcat Service, see "Performing Tomcat Service Procedures" section on page 1-2.	If you have purchased a license for the ops views feature, this box is checked by default.
Show Error Notifications	When checked, Cisco IPICS displays a notification message in the Administration Console when a fatal error occurs. This message displays in a red message pane at the top of the current window. This notification only appears in the current window for any user that has system administrator or All privileges in Cisco IPICS. When this box is unchecked, the notifications do not display. The system administrator or user who is defined in the All role would need to view the Recent System Log Entries pane in the System Status window to see any error messages. For more information about the System Status window, see the "The System Status Window" section on page 3-1	This feature is activated (the check box is checked by default).

Table 4-1 Option Window Settings and Controls (continued)

Setting	Description	Default Setting
Minimum Password Length	This setting specifies the minimum number of characters that a user can enter when creating or changing the Cisco IPICS password in the Administration Console User Profile window. Use the drop-down list to choose a new setting. The minimum length can range from 1 to 20 characters.	The default setting specifies 8 characters.
Minimum Digit Password Length	This setting specifies the minimum number of numeric characters that a user can enter when creating or changing the Digit Password in the Administration Console User Profile window. Use the drop-down list to choose a new setting. The minimum length can range from 1 to 10 characters.	The default setting specifies 4 characters.
Policy Scheduler Interval	The Policy Scheduler is a Cisco IPICS process that checks, at regular intervals, which policies should activate according to the current time. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value.	The default interval between checks specifies 600 seconds (10 minutes).
PMC Activity Log Update	The Cisco IPICS server gathers activity logs from the PMC client machines and updates the database with this information at regular intervals. In the Cisco IPICS database, this data is parsed, organized, and made available for queries from the Activity Log window of the Administration Console. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value.	The default update frequency specifies 600 seconds (10 minutes).

Table 4-1 Option Window Settings and Controls (continued)

Setting	Description	Default Setting
RMS Polling Frequency	Cisco IPICS includes an RMS polling process that checks, at regular intervals, whether the server can reach all of the RMS components that are listed in the Manage RMS window. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value.	The default interval between checks specifies 500 seconds (about 8 minutes).
Maximum Activity Logs	This setting specifies the maximum amount of hard disk space that may be used by Cisco IPICS activity logs. The Database % Full indicator is calculated according to this setting. For more information, see the "The System Status Window" section on page 3-1. This setting specifies a value in megabytes (MB). To change the default, double-click the current setting and enter a new value. The maximum space can range from 1 MB to 250 MB.	The default maximum space for activity logs specifies 50 MB.
PMC Send Logs on Rollover	Cisco IPICS defines the PMC UserInterface.log, Authentication.log, and ChannelStatistics.log log files based on a maximum size of 1MB. When any one of these log files reaches this predefined limit, the system creates a new log file. When you enable this option, the Cisco IPICS server retrieves the log files from the PMC based on file size rollover and renames the uploaded log file to reflect an archive copy. If you do not enable this option, the PMC deletes the log files when they reach their maximum size limit.	The PMC does not upload files on rollover (the check box is unchecked).

Table 4-1 Option Window Settings and Controls (continued)

Setting	Description	Default Setting
PMC Update Poll	The PMC application on the client machine receives updates from the server at regular intervals. For more information, refer to the *Cisco IPICS PMC Installation and User Guide*. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value.	The default polling interval specifies 5 seconds.

Table 4-1 Option Window Settings and Controls (continued)

Setting	Description	Default Setting
PMC Versions to Keep	Cisco IPICS provides new versions of the PMC application to client machines as soon as the versions are available. If the version that the server offers is newer than the latest version on the client machine, then the PMC user is given an option to download the version. This setting specifies the maximum number of versions (including the current version) that are maintained on the client machine. If the number of versions on the client machine exceeds this setting after a client downloads a new version, the oldest version is automatically deleted. For information about maintaining the PMC versions, refer to the *Cisco IPICS Server Administration Guide*. Use the drop-down list to choose a new setting. The setting can range from 1 to 10 versions.	The default setting specifies 3 versions.
PMC Log Upload Frequency (PMC to server)	When a PMC client has activity logs ready to upload to the Cisco IPICS server, the PMC application places the logs in a queue. At regular intervals, the PMC client checks the queue and uploads to the server any logs that are waiting to be uploaded. This setting specifies the interval between these checks. For more information, refer to the *Cisco IPICS PMC Installation and User Guide*. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value.	The default upload frequency specifies 600 seconds (10 minutes).

Troubleshooting the Cisco IPICS Server

The following sections describe how to resolve problems that you may encounter when you use the Cisco IPICS server and its components:

Browser Guidelines

When you access the Cisco IPICS Administration Console by using a browser, follow these guidelines:

- Windows in the Administration Console do not refresh automatically. As a best practice, make sure that you update your browser window often and before you perform any server administration functions to ensure that you are working with the most current information. If you attempt to perform an administration update 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 window displays the most up-to-date 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.
- To avoid browser-related memory issues, exit your browser and then restart it after prolonged use of the Cisco IPICS Administration Console.

Cisco IPICS Installation Issues

The issues that are described in this section may occur during or as a result of installing the Cisco Linux operating system or the Cisco IPICS server software. For information about troubleshooting the PMC application installation, see the "Generating a PMC Installation Log File" section on page 6-3.

This section includes the following topics:

Caution Cisco IPICS does not support any modification of the system date and time in the operating system after the Cisco IPICS software has been installed. As a best practice, make sure that you only perform system date changes before you install the Cisco IPICS software. If you change the system date to a past date, you will invalidate your Cisco IPICS license.

To resolve this situation, you must reset the system date to the current date and then upload the license file or restart the server. If you change the system date to a future date and then try to reset it to the current date, you will invalidate your license. To resolve this situation, you must reset the system date to the current date

and then restart the Cisco IPICS system. Make sure that you do not make repetitive changes to the system date. Changes to the system date can cause unexpected behavior, which may require you to reload your software. When you invalidate your license, Cisco IPICS displays a message, after you log in to the Administration Console, to inform you that your system does not have a valid license.

For information about changing the system date and time, refer to the *Cisco IPICS Server Installation Guide*.

No Ports Are Listed in the Network Device Control Window

Problem When you open the Network Device Control window to configure the Ethernet port, no ports are listed.

Solution During the Installation of Cisco Linux, you may have logged in with the system user ID and password that you created. For more information, refer to the *Cisco IPICS Server Installation Guide*.

To continue with the installation, you must log out and then log back in as the root user. To return to the Network Device Control window as the root user, perform the following procedure:

Procedure

Step 1 Close the current Network Device Control window by clicking **Close**.

Step 2 Before you can log in as root, you must log out as the system user. To log out, click the **Red Hat** menu and then choose **Log Out**.

The Log Out window displays.

Step 3 Choose **Log Out** and then click **OK**.

Cisco Linux logs you out and then displays a new login window.

Step 4 Enter **root** in the Username field and press **Enter**.

Step 5 Enter **cisco** in the Password field and press **Enter**.

Step 6 Open a terminal window to enter commands. To do so, open the Red Hat menu on the Cisco Linux desktop by clicking the **Red Hat** icon.

Step 7 Choose **System Tools > Network Device Control**.

The Network Device Control Menu displays and shows the Ethernet port(s) on the server.

Cannot Connect to the Server after Installation

Problem After you install Cisco IPICS, you enter the static IP address or the host name for the Cisco IPICS server into a browser and you cannot contact the server.

Solution If you cannot connect to the Cisco IPICS server through a browser, one of the following situations may have occurred:

- You entered the incorrect IP address for the Cisco IPICS server
- The Tomcat service is not running

To diagnose the problem, perform the following procedure:

Step 1 Check that you entered the correct IP address for Cisco IPICS into the browser.

If you still cannot connect to the Cisco IPICS server, continue to Step Step 2.

Step 2 Ensure that the Tomcat service is running. For information about checking the status of the Tomcat service, see the "Checking the Status of the Tomcat Service" section on page 1-2.

If the Tomcat service is not running. manually start the Tomcat service. For information about starting the Tomcat service, see the "Starting the Tomcat Service" section on page 1-5.

Step 3 If the Tomcat service was not running and you had to start it manually, follow these steps:

a. Check whether the cron was installed by searching for the tomcatcron file on the server. To check the existence of the tomcatcron file, enter the following command:

[root] **#crontab -l**

b. Take one of the following actions:

– If the crontab command returned a message such as "no crontab for root," install the tomcatcron file by entering the following command:

[root] **#crontab /opt/cisco/ipics/tomcat/cron_root**

Cisco IPICS starts the Tomcat service automatically after one minute. You can then log into the Administration Console through your browser, as usual.

- If there is no response from the crontab command, then the tomcatcron file already exists. For information about checking and, if necessary, editing the tomcatcron file, see the "Performing Tomcat Service Procedures" section on page 1-2.

Step 4 To verify that the static IP address, subnet mask and default gateway are properly configured, follow these steps:

a. To open a terminal window, click the **Red Hat** menu and choose **System Tools > Terminal**

b. Enter your root password and press **Enter**.

The Cisco Linux desktop displays.

c. To try to establish connectivity with the default gateway of another sever on the network, enter the following command:

ping <*default gateway IP address***>**

where *default gateway IP address* represents the default gateway address for your network.

d. If the ping command is successful, log in to another server on the network and attempt to ping this Cisco IPICS server.

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

Authorization Error after Installation

Problem After installing Cisco IPICS, you log into the Administration Console and receive an authorization error.

Solution An authorization error can occur in one of the following circumstances:

- You may have entered an incorrect user name or password
- The Informix database may not have started.

To resolve this problem, perform the following procedure:

Procedure

Step 1 Before you check the status of the Informix database, verify that you entered the correct user name and password, and that the Caps Lock setting is not on.

If you confirm that you entered the correct login information for the Cisco IPICS Administration Console and still receive an authorization error, you must check the status of the database. Continue to Step 2.

Step 2 To log into the Cisco Linux operating system on the Cisco IPICS server, enter **root** in the user name field of the Login window and press **Enter**.

Cisco Linux displays a window with a password field.

Step 3 Enter your root password and press **Enter**.

The Cisco Linux desktop displays.

Step 4 To open a terminal window, click the **Red Hat** menu and choose **System Tools > Terminal**

A terminal window displays.

Step 5 Enter the following command at the prompt:

[root] **#ps -ef | grep oninit**

If there is no response to the oninit command, then the Informix database is not running. Continue to Step 6.

If the database is running properly, the grep command returns a process similar to the following example. In this case, see the "Administration Console Does Not Function Properly" section on page 5-23.:

```
informix  5575     1  0 Oct26 ?        00:00:50
/opt/cisco/ipics/database/current/bin/oninit -r
root      5576  5575  0 Oct26 ?        00:00:08
/opt/cisco/ipics/database/current/bin/oninit -r
root      5577  5576  0 Oct26 ?        00:00:02
/opt/cisco/ipics/database/current/bin/oninit -r
root      5578  5576  0 Oct26 ?        00:00:00
/opt/cisco/ipics/database/current/bin/oninit -r
root      5579  5576  0 Oct26 ?        00:00:01
/opt/cisco/ipics/database/current/bin/oninit -r
root      5580  5576  0 Oct26 ?        00:00:00
/opt/cisco/ipics/database/current/bin/oninit -r
root     15750 15700  0 14:12 pts/1    00:00:00 grep oninit
```

Step 6 Manually start the Informix database by entering the following command at the prompt:

[root] **#/etc/init.d/ipics_db start**

Error Displays When Performing Remote Installation

Problem When you start the Cisco IPICS server software installation from an SSH Tectia Client window on a network PC, the installer displays an error similar to the following example:

Example 5-1 Remote Installation Error

```
Invocation of this Java Application has caused an
InvocationTargetException. This application will now exit. (LAX)

Stack Trace:
java.awt.HeadlessException:
No X11 DISPLAY variable was set, but this program performed an
operation which requires it.
        at java.awt.GraphicsEnvironment.checkHeadless(Unknown Source)
        at java.awt.Window.<init>(Unknown Source)
        at java.awt.Frame.<init>(Unknown Source)
        at java.awt.Frame.<init>(Unknown Source)
        at javax.swing.JFrame.<init>(Unknown Source)
        at com.zerog.ia.installer.LifeCycleManager.f(DashoA8113)
        at com.zerog.ia.installer.LifeCycleManager.g(DashoA8113)
        at com.zerog.ia.installer.LifeCycleManager.a(DashoA8113)
        at com.zerog.ia.installer.Main.main(DashoA8113)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown
Source)
        at java.lang.reflect.Method.invoke(Unknown Source)
        at com.zerog.lax.LAX.launch(DashoA8113)
        at com.zerog.lax.LAX.main(DashoA8113)
This Application has Unexpectedly Quit: Invocation of this Java
Application has caused an InvocationTargetException. This application
will now exit. (LAX)
```

Solution This error occurs when you invoke the installer file without the **-i console** argument. Ensure that you enter the following command:

[root] #**./<*name of installer file*>.bin -i console**

Communications Issues

The issues that are described in this section describe situations in which users have difficulty when communicating with other Cisco IPICS users. These situations may occur in a VTG or when a PMC user or Cisco IP Phone user communicates on a channel.

This section includes the following topics:

One Location Cannot Participate in VTG

Problem The multicast address for a PTT 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 The multicast address for the PTT channel is set to All, but the address may not be configured to reach everyone in the domain. The network administrator must reconfigure the router to include Location A. The problem might be, for example, an IP access list blocking that channel or a firewall setting, or that multicast is not configured properly.

For more information about multicast troubleshooting, see the *IP Multicast Troubleshooting Guide*.

Participants Cannot Communicate in VTG

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

Solution Check whether the Protocol Independent Multicast (PIM) is set to sparse mode on the router. If you set the router PIM to sparse mode and do not configure a rendezvous point (RP), the router will drop the packets and your VTG participants will not hear any audio. To ensure that this problem does not occur, perform one of the following tasks:

- Set the PIM to sparse-dense mode. If no RP is found, it automatically reverts to dense mode. To configure the router for sparse-dense mode, type the following commands in the router CLI:

  [router] **#configure terminal**

  [router (config)] **#interface <name of interface>**

  [router (config) interface name] **#ip pim sparse-dense-mode**

- Configure an RP manually and continue to use sparse mode.

For more information about multicast troubleshooting, see the *IP Multicast Troubleshooting Guide*.

Some PMCs Can Communicate on a Channel, but Other PMCs Cannot Communicate

Problem Several PMC users have successfully communicated on a channel. However, subsequent PMC users, after successfully logging in the same location and attempting to activate the same channel, could not listen or talk on the channel.

Solution The router that the channel is using does not have sufficient DSPs. For this channel to accommodate more PMC users, you must add more DSPs. If all the DSP slots are full, please make sure that the appropriate number of RMS time slots have been disabled.

Refer to the *Cisco IPICS Server Administration Guide* or the *IP Multicast Troubleshooting Guide* for more information.

PMC Voice Quality is Poor

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

Solution When you configure a channel, you have to 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 less DSP resources. Also, restrict the number of "remote" users with access to any channels or VTGs. Associate as few channels as needed.

Channel Automatically Deactivates on PMC

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.

Solution When this situation occurs, the PMC automatically reactivates the connection after 30 seconds. Alternatively, you can reactivate the channel by clicking the **Activate** button on the PMC.

Note If the PMC user activates several channels, the timing to deactivate is separate for each channel.

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) **#timer receive-rtcp 5**

For more information about proper router configuration for Cisco IPICS, refer to the *Cisco IPICS Server Administration Guide*.

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

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 machines 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 Differentiated Service Code Point (DSCP) to ensure the highest priority handling when the packets are transmitted between end points. When incorrectly marked packets are dropped or lost, voice quality degrades.

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.

Feedback Noise on VTG

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

Solution This problem occurs when the audio from the conference plays through the microphone of a user who is talking in the conference. For example, this might happen if you are listening to a PTT 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). This can create various types of feedback noise, including metallic echoes or whistling noises.

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

Equipment Issues

The issues that are in this section describe problems that you may encounter with the Cisco IPICS hardware. For issues that relate to communication difficulties, see the "Communications Issues" section on page 5-8.

This section includes the following topics:

Voice Communications are Interrupted When You Use VTGs and SIP-Connected PMCs

Problem Voice communications may be interrupted when you use VTGs and SIP-connected PMCs when certain commands are not included in the T1 controller configuration. 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.

Cisco IPICS also requires that you configure the clock source of a T1 link to ensure synchronization.

To resolve this issue, perform the following procedure:

Procedure

Step 1 Log in to the router.

Step 2 From the router prompt, enter the following command in controller configuration mode:

[router] **#cablelength short 133**

This command specifies a cable length from 0 to 133 feet.

Step 3 Configure the clock source on only one of the T1 controllers in the loopback by entering the following command:

[router] **#clock source internal**

This command specifies that clock is generated from the T1 controller's internal phase-locked loop (PLL).

Step 4 On the other T1 controller in the loopback, enter the following command:

[router] **#no clock source**

This command specifies that there is no clock source on this T1 controller.

Note Make sure that you specify the correct clock source for each T1 controller. See Example 5-2 for an example of the configuration for the two controllers.

Step 5 Clear the error counters with the **clear counters** command.

Step 6 Make sure that you check the T1 controller configuration on a regular basis. To display information about the T1 controllers, use the show controllers T1 command in privileged EXEC mode.

[router] **#show controllers T1**

The output from the command displays. Example 5-3 shows the output from the sample configuration from Example 5-2.

Example 5-2 Sample Configuration for Two T1 Controllers

```
controller T1 1/0/0
  framing esf
  clock source internal
  linecode b8zs
  cablelength short 133
  ds0-group 0 timeslots 24 type e&m-lmr
  ds0-group 1 timeslots 1 type e&m-lmr
  ds0-group 2 timeslots 2 type e&m-lmr
  ds0-group 3 timeslots 3 type e&m-lmr
  ds0-group 4 timeslots 4 type e&m-lmr
  ds0-group 5 timeslots 5 type e&m-lmr
  ds0-group 6 timeslots 6 type e&m-lmr
  ds0-group 7 timeslots 7 type e&m-lmr
  ds0-group 8 timeslots 8 type e&m-lmr
  ds0-group 9 timeslots 9 type e&m-lmr
  ds0-group 10 timeslots 10 type e&m-lmr
  ds0-group 11 timeslots 11 type e&m-lmr
  ds0-group 12 timeslots 12 type e&m-lmr
  ds0-group 13 timeslots 13 type e&m-lmr
  ds0-group 14 timeslots 14 type e&m-lmr
  ds0-group 15 timeslots 15 type e&m-lmr
  ds0-group 16 timeslots 16 type e&m-lmr
  ds0-group 17 timeslots 17 type e&m-lmr
  ds0-group 18 timeslots 18 type e&m-lmr
  ds0-group 19 timeslots 19 type e&m-lmr
  ds0-group 20 timeslots 20 type e&m-lmr
  ds0-group 21 timeslots 21 type e&m-lmr
  ds0-group 22 timeslots 22 type e&m-lmr
  dso-group 23 timeslots 23 type e&m-lmr

controller T1 1/0/1
  framing esf
  linecode b8zs
  cablelength short 133
  ds0-group 0 timeslots 24 type e&m-lmr
  ds0-group 1 timeslots 1 type e&m-lmr
  ds0-group 2 timeslots 2 type e&m-lmr
  ds0-group 3 timeslots 3 type e&m-lmr
  ds0-group 4 timeslots 4 type e&m-lmr
  ds0-group 5 timeslots 5 type e&m-lmr
  ds0-group 6 timeslots 6 type e&m-lmr
  ds0-group 7 timeslots 7 type e&m-lmr
  ds0-group 8 timeslots 8 type e&m-lmr
  ds0-group 9 timeslots 9 type e&m-lmr
  ds0-group 10 timeslots 10 type e&m-lmr
  ds0-group 11 timeslots 11 type e&m-lmr
```

```
  ds0-group 12 timeslots 12 type e&m-lmr
  ds0-group 13 timeslots 13 type e&m-lmr
  ds0-group 14 timeslots 14 type e&m-lmr
  ds0-group 15 timeslots 15 type e&m-lmr
  ds0-group 16 timeslots 16 type e&m-lmr
  ds0-group 17 timeslots 17 type e&m-lmr
  ds0-group 18 timeslots 18 type e&m-lmr
  ds0-group 19 timeslots 19 type e&m-lmr
  ds0-group 20 timeslots 20 type e&m-lmr
  ds0-group 21 timeslots 21 type e&m-lmr
  ds0-group 22 timeslots 22 type e&m-lmr
  dso-group 23 timeslots 23 type e&m-lmr
```

The following example shows the output from running the **show controllers** command with the configuration from Example 5-2.

Example 5-3 Sample Output from the show controllers Command

```
router_1#show controllers T1
T1 1/0/0 is up.
  Applique type is Channelized T1
  Cablelength is short 133
  No alarms detected.
  alarm-trigger is not set
  Version info Firmware: 20041023, FPGA: 16, spm_count = 0
  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
   Current port master clock:recovered from T1 1/0/1
  Data in current interval (250 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail
Secs
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     19555 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded
Mins,
     19555 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0
Unavail Secs
T1 1/0/1 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db   <-- This is what it shows if the
cablelength command is missing.
  No alarms detected.
  alarm-trigger is not set
  Version info Firmware: 20041023, FPGA: 16, spm_count = 0
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
   Current port master clock:recovered from T1 1/0/1
```

```
  Data in current interval (262 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail
Secs
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     19554 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded
Mins,
     19554 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0
Unavail Secs
```

For more information about the proper configuration for routers that you use with Cisco IPICS, refer to the *Cisco IPICS Server Administration Guide*.

No Power to Cisco IP Phones

Problem Cisco IP Phones are not receiving power.

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

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

Note For information about the proper IOS software versions for the Cisco IP Phones that Cisco IPICS supports, refer to the *Cisco IPICS Hardware Compatibility Matrix*.

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

[router] **#show power**

- If the command returns an “unsupported command” message, for example, the IOS software version is incorrect. Installing the correct IOS version would probably correct the problem.
- If the command returns information about the power, the cause of the problem is probably the lack of a POE power module.

  To work around this issue, either use wall sockets for power or install POE in the router.

Router Configuration Issues

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

This section includes the following topics:

Long Wait After Restarting Cisco IPICS Following RMS Configuration

Problem Restarting Cisco IPICS takes almost two minutes.

Solution After you define one or more RMS components for which you have allocated a large number of DS0 voice ports, Cisco IPICS may restart slowly.

When you restart Cisco IPICS, the server verifies that all of the RMS components are still operational and match the last configured condition for the RMS. This verification is necessary, because the RMS components may have also restarted.

At this time, Cisco IPICS also reconfigures all of the DS0s to match the last known state in the configuration data. If an RMS has, for example, 96 DS0s, then Cisco IPICS must send anywhere from 800 to 1400 commands to the router. On higher performing routers, this may take 10 to 20 seconds. On lower performing routers, this process may take one to two minutes (60 to 120 seconds).

To solve this problem, use a higher performing router, such as the Cisco 3845 rather than a model such as the Cisco 3725. Also, do not heavily load any RMS with controllers and DS0s.

Cisco recommends that you limit an RMS to approximately 6 controllers with a total of approximately 100 DS0s.

VTG Activation Slow or RMS in Unreachable State

Problem Activation of VTGs is slow, remote user logins are slow or frequently exhibit errors, or the RMS is frequently or persistently in an Unreachable state.

Solution If you change the prompt on the router, either before or after you add the RMS component to Cisco IPICS, operations such as VTGs activation and deactivation may fail.

Cisco IPICS only supports the default prompts.

To avoid problems, keep the default prompt by using the **no prompt** router configuration command.

RMS Fails or Remains in Unreachable State

Problem The RMS fails or remains in an unreachable state and you can observe the following information:

- All virtual teletype interface (VTY) lines are in use.
- The ipics.log file includes the following error message:

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

Solution This problem may occur when multiple Cisco IPICS users are logged in to the router and have used all of the available VTY lines. In this situation, the Cisco IPICS server cannot communicate with the router.

To verify that all of the VTY lines are in use, use the Telnet or use a Secure Shell (SSH) command to access the router. Then, enter the **show users** command to display information about the lines that are active on the router.

To clear a VTY line, enter the **clear line** command. (This command terminates the service on the specified line and closes any open files.)

To help resolve this problem, you can configure a time interval that the VTY lines wait for expected user input. To configure this interval, set the exec-timeout interval to 22 minutes. Be sure to save any configuration changes that you make.

You can also limit the number of users who can log in to any router that you use with Cisco IPICS.

New RMS Does Not Display Loopbacks

Problem The RMS that you added to Cisco IPICS does not display loopbacks in the Edit Router Details area of the Administration Console.

Solution You may have attempted to add an RMS with a partial or unsupported controller configuration.

Refer to the *Cisco IPICS Server Administration Guide* for proper configuration information.

Router Remains in Unreachable State

Problem After updating the login information to an RMS, you cannot access it from the Cisco IPICS server. In the Administration Console Manage RMS window, the RMS displays as Unreachable.

Solution You may have activated the RMS with incorrect settings, such as a user name, password, or IP address. This causes the RMS to enter an unreachable state, without any way to fix the incorrect settings or to disable the RMS.

This situation occurs 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 In the Manage RMS window of the Administration Console, select the router and click **Details**.

The Edit Router Details area displays.

Step 2 Deactivate the router by clicking **Deactivate**.

The router displays with an Out of Service state.

Step 3 Enter the correct username and password for the router in the Edit Router Details area.

Step 4 Click **Save**.

Step 5 Reactivate the router by clicking **Reactivate**.

If the username and password you entered are correct, the router reactivates and displays with an Operational state.

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 are not on.

Solution Each set of ports on the router has the following indicator lights. Check the loopbacks on your router to see which of the following indicator lights is on:

- Alarm Indication (AL)—This red light indicates one of the following problems:
  - 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)—This yellow light indicates one of the following problems:
  - The cable has a loose connection
  - The cable is defective
- Both the Alarm Indication (AL) and Carrier Detect (CD) lights are on
  - The interface is shutdown—Enable the interface by executing the **no shutdown** command on both ends of the T1 loopback interface
  - 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 B8ZS encoding standard on both ends of the loopback
- Carrier Detect (CD)—This green light indicates that there are no problems with the loopback.

Voice Loops in Conferences and Router Configuration Shows Incorrect Information

Problem Users experience voice loops (continuous echoes) in conferences. The Show Configuration feature in the Manage RMS window displays settings for voice ports or dial peers that are not currently in use.

Solution When you add an RMS to a Cisco PICS system, particularly an RMS that was previously associated with another Cisco IPICS system, you may observe differences between the "Show Configuration" and the configuration in the RMS Details area. 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.

Cisco IPICS automatically updates an RMS every 10 minutes with the configuration that you can view in the RMS Details area. After you make a change to a new RMS, such as adding loopbacks, the RMS configuration is not updated until the monitor process has a chance to run.

To ensure that the Cisco IPICS configuration and the configuration on the RMS are in sync, you can click **Update Configuration** after you add an RMS (or after you add loopbacks to a previously configured RMS. This rewrites all of the voice resources with the current status. Alternately, you can simply wait for up to 10 minutes and Cisco IPICS will automatically update the RMS.

Note When you click **Update Configuration**, any currently active voice resources on the RMS will be reconfigured and this action may cause a momentary loss of connection.

General Operation Issues

The issues listed in this section describe situations that users may encounter in using the Cisco IPICS Administration Console.

This section includes the following topics:

Administration Console Does Not Function Properly

Problem Users cannot log in to the Administration Console from the Login window. Users who are currently logged in to the system encounter errors when they try to perform tasks. Existing conferences (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
- The informix user password has changed

If the database has stopped or gone into quiescent mode, you can perform procedures to start the database again. However, if the informix password was manually changed, the Cisco IPICS server will not be able to access the database until you reset the password by reinstalling the Cisco IPICS server software.

Caution When you manually change the informix password, Cisco IPICS can no longer process commands to the database. Make sure that you do not change the informix password unless you are prompted to do so by the Cisco IPICS installation or upgrade procedure.

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. Log in to the server as root by entering root in the Login window user name field; then press **Enter**.

Cisco Linux displays a window with a password field.

b. Enter your root password and press **Enter**.

The Cisco Linux desktop displays.

c. Open a terminal window by clicking the **Red Hat** menu and choose **System Tools > Terminal**.

A terminal window displays.

d. From root, enter the following command:

[root] **#onstat –l**

If the database is online and running, the command returns the following response; continue to Step 3.

```
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 e.

```
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; start the database:

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

For information about starting the database, see the "Starting the Informix Database" section on page 1-10.

e. If the database is in quiescent mode and a restore operation is in progress, wait for the operation to complete.

If you are not currently restoring the database, the database may have stopped in maintenance mode. To move the database into online mode, enter the following command:

[root] **#onmode –m**

f. Check to see if the database is running by entering the following command at the prompt:

[root] **#onstat –l**

Take one of the following actions:

- If the response to the command indicates that the database is online, continue to use Cisco IPICS as normal.
- If the command returns any other response, you may need to terminate the database processes before you can start the database again. For more information, see the "Stopping the Informix Database" section on page 1-9.

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

[root] **#/etc/init.d/ipics_db start**

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

If the database does not successfully start, check the diagnostics.log file, which is located in the following directory:

/opt/cisco/ipics/database/logs

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

Step 3 If the database is running properly and you cannot use the Administration Console, check the informix user password to make sure that it was not manually changed.

Caution When you manually change the informix password, Cisco IPICS can no longer process commands to the database. Make sure that you do not change the informix password unless you are prompted to do so by the Cisco IPICS installation or upgrade procedure.

The only method for resetting the informix user password for Cisco IPICS is to reinstall the Cisco IPICS server software. During the procedure, you create a new password for the informix user. For information about performing a Cisco IPICS server installation, refer to the *Cisco IPICS Server Installation Guide*.

Note If you must reinstall the Cisco IPICS server software to resolve the issue, notify users that communications will be disrupted until the installation process has completed.

Database Full Message Displays and Users Cannot Save Data

Problem When I click **Save** (in any window in the Administration Console), Cisco IPICS displays a message that the database is full.

Solution The logical logs may be full, due to an extremely high amount of activity on the system. You can verify the amount of database consumption for the logical logs in the System Status window in the Administration Console. If the Database % Full indicator displays that the database is full, you can purge the logs by clicking **Purge**.

For more information about the Purge feature, see the "Purging Activity Logs from the Database" section on page 3-4.

VTG Activates by Itself

Problem As a dispatcher, I see in the VTG Workspace that a VTG activated, but I did not click **Activate**.

Solution One of the following may have occurred:

- The VTG was triggered by a policy. Check the Manage Policies window to see which policy(s) contained that VTG.
- Another dispatcher is logged into 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.

Policy Is Active But VTG Is Not

Problem The Manage Policies window shows me that a policy is active, but the one of VTGs in the policy was not activated.

Solution The system may have insufficient resources, such as no available 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 does not have more than two available multicast addresses).

User Added to VTG, but No VTG Appears 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 in the database under two different user IDs. The user may log in with one name, while the operator or dispatcher use another ID for the user.

Check the Users list in the Manage Users window for duplicate user entries and delete any unused IDs.

Cisco IP Phone Cannot Access Channel

Problem A Cisco IP Phone cannot access a channel that was associated to it.

Solution The location information may be incorrectly configured. Check your user profile in the Cisco IPICS Administration Console (see the *Cisco IPICS Server Administration Guide* for more information) or contact your operator.

The Cisco IPICS server does not allow Cisco IP Phone users who are remote from the PTT channel. When the user is remote to the channel, the channel does not appear or is not selectable for the user on the Cisco IP Phone.

VTGs and Policies Not Functioning Properly

Problem Problems are occurring in the Administration Console. For example, the dispatcher cannot activate policies and VTGs.

Solution To troubleshoot these problems, you should change a setting in the log4j.properties file to set the file to collect debugging information. When you do this, the ipics.log file, which you can view and download in the Administration Console System Status window, begins collecting debug information. You can use this to collect helpful information about this issue.

To begin collecting debug information, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root privileges.

Step 2 Open a terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

Step 3 To stop the Tomcat service by entering the following command:

[root] **/etc/init.d/ipics_tomcat stop**

Step 4 Open the file for editing by entering the following command:

[root] **#vi /root/tomcat/current/webapps/ipics_server/WEB-INF/classes/log4j.properties file**

Step 5 Locate the following setting in the file:

log4j.logger.com.cisco.ipics.server

Step 6 Change the setting from info to debug.

Step 7 Save and close the file with the **:wq** command.

Step 8 Restart the Tomcat service by entering the following command:

[root] **/etc/init.d/ipics_tomcat start**

Step 9 Exit the terminal window by clicking **X**.

Caution Setting the log4j.properties file to debug can generate a large number of messages during periods of high traffic. Be sure to change the setting back to info after you finish debugging.

Browser Displays 404 Error for Cisco IPICS

Problem When trying to access the Cisco IPICS in the browser, I received the following error:

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

In the Administration Console System Status window, the entries in the ipics.log file include the following message:

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

Solution A portion of the Cisco IPICS system has been corrupted.

To correct the problem, perform the following procedure:

Step 1 Log into the server as the root user.

Step 2 Delete the ipics_server folder with the following command:

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

Step 3 Restart tomcat with the following command:

[root] **#/etc/init.d/ipics_tomcat restart**

Cisco Linux responds with a message, indicating whether the Tomcat server has started.

When you restart the Tomcat server, the ipics_server.war file recognizes that the ipics_server folder is missing and expands to create another.

Step 4 Open a browser and enter the address for Cisco IPICS.

Some Windows Display No Data and an Undefined Error

Problem Some Internet Explorer browser users may receive a javascript "undefined" error and not see any data display in Administration Console windows that display data in a table format. This problem occurs when the IE browser javascript engine cannot handle advanced dynamic features because of installation of third party software or other setup issues.

Solution 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.

Intermittent Commands Fail

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 Commands that Cisco IPICS sends to the RMS fail for no apparent reason. This may occur during VTG activation or deactivation or when a PMC user logs in or logs out.

When the problem occurs, you can find an error in the ipics.log and/or the ipics.rms.log file.

This problem is intermittent, however, and you can work around it by simply trying the command or action again.

Backup Log Displays Incorrectly in Notepad

Problem When I download the backup log in the Manage Database window and choose Open, Notepad displays the file as one continuous text block.

Solution The backup log you download from the Manage Database window is the bar_act.log, which includes UNIX newline characters. These characters cannot be read in Notepad or any editor that only reads plain text.

To resolve this problem, perform the following procedure:

Procedure

Step 1 When you download the log file from the Manage Database window, click **Save** to save the file to your PC.

Step 2 Choose a location on your PC to save the file and click **Save**.

Step 3 Open a Desktop Explorer window and navigate to location where you saved the bar_act.log file.

Step 4 Right-click the file and choose **Open with > Choose Program**.

Step 5 Choose WordPad or another text view that is capable of reading UNIX newline characters.

Some Language Characters Display Incorrectly

Problem Some information, such as user names and PTT 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 From the Internet Explorer menu, choose **Tools > Internet Options**.

The Internet Options window displays.

Step 2 Click **Fonts**.

The Fonts dialog box displays.

Step 3 From the Web page font pane, select Arial Unicode MS.

Step 4 To accept the font choice, click **OK**. Then, click **OK** to save your changes and close the Internet Options window.

Internet Explorer now displays the languages correctly.

PMC Users Receive Error Message After Database Restore

Problem After a database restore procedure has been completed, 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 is not restarted after the restore procedure is 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 Verify if the Tomcat service is running. For more information, see the "Checking the Status of the Tomcat Service" section on page 1-2.

Step 2 If the Tomcat service is not running, start it. For more information, see the "Starting the Tomcat Service" section on page 1-5.

If the Tomcat service is running, wait for at least 5 minutes so that the database has time to synchronize its information with the RMS.

Step 3 If you continue to experience problems, check the ipics.log file, which is located in the **/opt/cisco/ipics/tomcat/versions/5.5.9/logs** directory.

Troubleshooting 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

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

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, perform the following 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 *Cisco IPICS PMC Installation and User Guide*.

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.

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 *Cisco IPICS PMC Installation and User Guide* 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.

Configuring the Audio Settings

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

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.

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 *Cisco IPICS PMC Installation and User Guide*.

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 *Cisco IPICS PMC Installation and User Guide* 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 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.

Refer to the *Cisco IPICS PMC Installation and User Guide* for detailed information about the audio setting configuration and sound recording capability.

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/univercd/cc/td/doc/product/vpn/ciscosec/csa/index.htm

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. Windows 2000, however, does 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 Windows 2000 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 Headset Issues, page 6-9
- Resolving IP Address Changes, page 6-10

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.

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, perform the following 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 the *Cisco IP Interoperability and Collaboration System Software Development Kit Guide*.

Using the CLI Play Command to Resolve 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 8, 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 IP Interoperability and Collaboration System Software Development Kit Guide*.

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

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

Troubleshooting PMC Connectivity Issues

The following topics provide information about troubleshooting PMC connectivity issues:

- Troubleshooting VPN Connectivity, page 6-12
- Using the PMC with the Windows XP Firewall, page 6-15
- Troubleshooting Multicast Communications Issues, page 6-16
- Troubleshooting Winsock Corruption Issues, page 6-17

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 6-13
- Enabling and Disabling the Stateful Firewall on the PMC Client Machine, page 6-14

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 > Express** 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 *Cisco IPICS PMC Installation and User Guide*.

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/univercd/cc/td/doc/product/vpn/client/index.htm

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/univercd/cc/td/doc/product/vpn/client/index.htm

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 following protocols:

- Internet Control Message Protocol (ICMP) type 8 (echo request) / ICMP type 0 (echo reply)
- Hypertext Transfer Protocol (HTTP) GET port 80 / HTTP/1.1 (response version 1.1)
- Hypertext Transfer Protocol Secure (HTTPS) port 443 and port 443 setup
- Standard Session Initiation Protocol (SIP) call setup

Contact your system administrator if you need assistance with your specific client machine configuration.

For more information about the Windows XP firewall, see the Microsoft support site at http://support.microsoft.com/.

Troubleshooting Multicast Communications Issues

Certain PMC client machines that are running the Windows 2000 and Windows XP operating systems may not be able to send multicast communications because of an issue with the operating system; in these situations, PMC multicast users may 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 *Cisco IPICS PMC Installation and User Guide*.

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 transmit traffic indicator LED blinks.)
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 2000 or 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.

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, the PTT button will not highlight.

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.

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 *Cisco IPICS PMC Installation and User Guide*.

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 always logs in to the same Cisco IPICS server that has been configured as the default server and from which the PMC was downloaded as part of the installation. To change servers, the PMC application must be reinstalled from a different Cisco IPICS server.
- Refer to the *Cisco IPICS PMC Installation and User Guide* for information about using the PMC in offline mode and PMC skin caveats.

Analyzing PMC Error Conditions

This section includes information about identifying and resolving errors that you may encounter when you use the PMC.

This section includes the following topics:

Cannot Connect to the Cisco IPICS server

Problem 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.

Solution Invalid entries in the pmc.ini file may be the cause of this problem. To check this file, perform the following steps:

Step 1 Navigate to **C:\Program Files\Cisco Systems\Cisco IPICS\PMC**.

Step 2 Search for the **pmc.ini** file.

Step 3 Right-click **pmc.ini** and click **Open With**.

Step 4 Click **Notepad**; then, click **OK**.

Step 5 Delete all entries in this file except the following fields: server_host, server_port, and server_port_ssl.

Step 6 Validate that the configured values in these fields are correct.

Note Contact your system administrator if you are not sure of these values or if these values are correct and you still cannot connect.

Can Receive But Not Transmit

Problem You can hear other users but they cannot hear you.

Solution Check your audio settings to make sure that your microphone is not set to mute. Refer to the *Cisco IPICS PMC Installation and User Guide* for more information about audio settings.

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.

Error Message When Trying to Download PMC

Problem 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.

Solution This problem may occur if the pmcsetup.exe file was erroneously modified, moved, renamed, or deleted from the server. Contact your system administrator for assistance.

Transmissions Sound Choppy

Problem When you talk, other users tell you that your voice sounds choppy and breaks up at times during a conversation.

Solution If Voice Activity Detection (VAD) is enabled, disable the setting in the Channels menu. Refer to the *Cisco IPICS PMC Installation and User Guide* for more information about VAD.

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.

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.

Volume Is Low on Voice Transmission

Problem When you talk, other users tell you that your voice sounds low.

Solution If your microphone gain is set too low, VAD may be interfering with and disabling output; this activity can result in choppy voice quality.

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.

Invalid User/password Error on Login

Problem When you attempt to log in to the PMC, you see an error message that states “invalid user or password.”

Solution 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.

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.

PMC Cannot Register with Cisco IPICS server

Problem 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.

Solution Upon initial connection to the server, the PMC must be able to register with the Cisco IPICS server to obtain its unique PMC ID.

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.

If the PMC continues to display this error message, contact your system administrator for assistance.

Security Alert for a Server Certificate

Problem The PMC displays a security alert dialog box that prompts you to approve the server certificate.

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.

Solution 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.

Cannot Access Media Devices Error

Problem When you try to launch the PMC, an error message displays because the PMC cannot access the media device.

Solution 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. Windows 2000, however, does not provide support for this same capability.

You may encounter this error if you are using Windows 2000 and 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.

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide*
- *Cisco IPICS Server Administration Guide*
- *Cisco IP Interoperability and Collaboration System Software Development Kit Guide*

Changing the Cisco Linux Root Password

You can change the password for the Cisco Linux root user, as needed, by performing the following procedure:

Note Your new password must be a minimum of six characters and cannot be based on a dictionary word.

Procedure

Step 1 Log in to the Cisco IPICS server with root privileges.

The Cisco Linux desktop displays.

Step 2 Open a terminal window by clicking the Red Hat menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 To temporarily disable the Cisco Linux restrictions for changing the root password, enter the following command:

[root] **#sh /root/.security/unimmunize.sh**

Step 4 To create a new root password, enter the following command:

[root] **#passwd**

Cisco Linux informs you that it is changing the password for the root user.

Step 5 At the New Password prompt, enter a new root password and press **Enter**.

When you enter your password, no characters display for security reasons.

Step 6 At the Retype New Password prompt, enter the new password again and press **Enter**.

Step 7 Upon password confirmation, the system displays the following message:

```
passwd: all authentication tokens updated successfully.
```

Step 8 To reenable the Cisco Linux restrictions for changing the root password, enter the following command:

[root] **#sh /root/.security/immunize.sh**

Step 9 Close the terminal window by clicking **X**.

You are returned to the Linux desktop.

A

activated — A VTG state that indicates that the SIP (unicast) line or multicast line is fully operational. The PTT and volume indicators appear highlighted.

activating — 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.

activation button — 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.

active virtual talk group — 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.

Administration Console — 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.

autonomous system — A radio system under one administrative control; also known as a management domain. This system is usually mapped to an agency.

B

backward compatibility — 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.

bandwidth 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.

base station 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

CAI 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.

call delay 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.

call setup time The time that is required to establish a circuit-switched call between users or terminals.

carrier A wave that is suitable for modulation by an information-bearing signal.

CAS 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.

channel 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. *See* PTT channel.

channel capacity The maximum possible information transfer rate through a channel, subject to specified constraints.

channel folder A logical grouping of channels

channel spacing The distance from the center of one channel to the center of the next-adjacent-channel. Typically measured in kilohertz.

Cisco CallManager The software-based call-processing component of the Cisco IP telephony solution. Cisco CallManager extends enterprise telephony features and functions to packet telephony network devices, such as Cisco IP Phones, media processing devices, VoIP gateways, and multimedia applications.

Cisco IPICS 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.

Cisco IPICS server 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.

Cisco IP Phone 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 IP Phone as a PTT device.

Cisco Security Agent Provides threat protection for server and desktop computing systems (endpoints) by identifying, preventing, and eliminating known and unknown security threats.

CLI command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments.

codec coder-decoder.

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.

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.

conference of conferences A conference that consists of two or more VTGs.

conventional radio system A non-trunked system that is similar to telephone party-line in that the user determines availability by listening for an open channel.

COR carrier operated relay. A signal from a receiver that indicates that the receiver is receiving a signal and that the receiver is not squelched.

coverage 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

delay time The sum of waiting time and service time in a queue.

decrypt Cryptographically restore ciphertext to the plaintext form it had before encryption.

decryption Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state.

dial peer Addressable call endpoint. In Voice over IP, there are two kinds of dial peers: POTS and VoIP.

digital ID 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 IP Phone user.

digital modulation technique A technique for placing a digital data sequence on a carrier signal for subsequent transmission through a channel.

dispatcher The Cisco IPICS dispatcher is responsible for setting up the VTG templates, activating the VTGs to begin conferences, and adding and/or removing participants in VTG templates and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute users, as necessary, and sets up system policies.

DS0 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.

dynamic regrouping 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

E & M recEive and transMit (or ear and mouth). The E&M interface provides voice signals from radio channels, which are then mapped to IP multicast or unicast. The E&M interface provides the most common form of analog trunking.

1. Trunking arrangement that is generally used for two-way switch-to-switch or switch-to-network connections. Cisco's analog E&M interface is an RJ-48 connector that allows connections to PBX trunk lines (tie lines). E&M also is available on E1 and T1 digital interfaces.

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.

encipher To convert plain text into an unintelligible form by using a cipher.

encode To modify information into the required transmission format.

encryption Application of a specific algorithm so as to alter the appearance of data and make it incomprehensible to unauthorized users.

event An active VTG in the Cisco IPICS solution.

F

FDM frequency-division multiplexing. Technique whereby information from multiple channels can be allocated bandwidth on a single wire based on frequency.

FDMA frequency-division multiple access. A a channel access method in which different conversations are separated onto different frequencies. FDMA is employed in narrowest bandwidth and multiple-licensed channel operations.

FLEXlm Cisco software that enforces licensing on certain systems; FLEXlm ensures that Cisco IPICS software will work only on the supported and licensed hardware.

floor control The standard mechanism for Push-to-Talk speaker arbitration.

frame 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.

frequency For a periodic function, frequency represents the number of cycles or events per unit of time.

frequency assignment Assignment that is given to a radio station to use a radio frequency or radio frequency channel under specified conditions.

frequency hopping The repeated switching of frequencies during radio transmission according to a specified algorithm, intended to minimize unauthorized interception or jamming of telecommunications.

frequency modulation Modulation technique in which signals of different frequencies represent different data values.

frequency sharing 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.

G

gateway 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.

GRE 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.

H

H.323 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.

high-band frequency Refers to the higher frequency levels in the VHF band, typically 138-222 MHz.

Hoot 'n' Holler (Hootie) 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.

i

I

inactive VTG A VTG that is stored for use. The Cisco IPICS server stores inactive VTGs so that they can be automatically activated by a policy or manually activated by a dispatcher.

incident management framework 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.

interference 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.

interoperability The capability of equipment manufactured by different vendors to communicate with each other successfully over a network.

IPSec 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.

K

keepalive 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.

key The parameter that defines an encryption code or method.

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.

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.

location 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.

low-band frequency Lower frequency levels in the VHF band, typically 25–50 MHz.

M

megahertz (MHz) A unit of frequency denoting one million Hz.

modulation The process, or result of the process, of varying a characteristic of a carrier in accordance with an information-bearing signal.

multicast 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.

multicast address A single address that may refer to multiple network devices.

multicast address/port Cisco IPICS uses this type of connection to enable the PMC to directly tune in to the multicast channel.

multicast pool 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.

multiplexing 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).

mute This 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.

mutual aid channel 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

narrowband channels Channels that occupy less than 20 kHz.

National Public Safety Planning Advisory Committee The committee that was established to conduct nationwide planning and allocation for the 821–824 MHz and 866–869 MHz bands.

National Telecommunications and Information Administration 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.

network An interconnection of communications entities.

NAT Network Address Translation. Provides a mechanism for translating addresses that are not globally unique into globally routable addresses for connection to the Internet.

not activated 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.

O

offline mode 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.

operator The Cisco IPICS operator is responsible for setting up and managing users, configuring access privileges, and assigning user roles and ops views.

ops view 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. While ops views are maintained separately by the Cisco IPICS system 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.

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.

PIM sparse mode 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.

PMC 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 VTGs at the same time.

PMC ID 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.

policy An association of events or triggers to an action. Policies can include a set sequence of actions, such as activating VTGs.

policy channel 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.

portalization A web programming paradigm for customizing the interface and functionality of a client application.

protocol A set of unique rules that specify a sequence of actions that are necessary to perform a communications function.

PTT Push-to-talk. A signal to a radio transmitter that causes the transmission of radio frequency energy.

PTT channel 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.

PTT channel button 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.

PTT channel group A logical grouping of available PTT channels that can be used for categorization.

Q

QoS quality of service. A measurement of performance for a transmission system, including transmission quality and service availability.

queue 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.

queuing delay 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

radio channel 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.

radio equipment 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.

receive indicator The indicator on the PMC that blinks green when traffic is being received.

remote connection Cisco IPICS uses this type of connection to provide SIP-based trunking into the RMS component, which is directly tuned into the multicast channel.

RF 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.

RF repeater 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.

RMS 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. The RMS mixes multicast channels in support of VTGs and it mixes remote 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.

RTP Real-Time Transport Procotol. Commonly used with IP networks to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services.

S

scanning 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.

SDM Security Device Manager. A web-based integrated router application, provides a user-friendly GUI for configuring security features in Cisco routers. Cisco IPICS uses SDM to configure voice ports and LMR functions on LMR gateways.

secure flag A PTT channel indicator that identities a channel as a secure PTT channel.

service delivery area *See* coverage.

signal The detectable transmitted energy that carries information from a transmitter to a receiver.

skin 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.

speaker arbitration The procedure that is used to determine the active audio stream in a Push-to-Talk system.

spectrum The usable radio frequencies in the electromagnetic distribution. The following frequencies have been allocated to the public safety community:

High HF 25–29.99 MHz
Low VHF 30–50 MHz
High VHF 150–174 MHz
Low UHF 406.1–420/450–470 MHz
UHF TV Sharing 470–512 MHz
700 MHz 764–776/794–806 MHz
800 MHz 806–824/851–869 MHz.

squelch An electric circuit that stops input to a radio receiver when the signal being received is too weak to be anything but noise.

stored VTG Also referred to as inactive VTG.

subscriber unit A mobile or portable radio unit that is used in a radio system.

system administrator 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.

system architecture 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.

T

T1 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.

T1 loopback 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.

talk group 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.

TCP 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.

TDMA 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.

terminal A device capable of sending, receiving, or sending and receiving information over a communications channel.

throughput The number of bits, characters, or blocks passing through a data communications system, or a portion of that system.

TIA/EIA-102 standards A joint effort between government and industry to develop voice and data technical standards for the next generation of public safety radios.

tone control The process of sending a 2175 Hz inband tone with voice transmission to control receiving radios remotely. An inband tone can be used to control functions such as frequency selection and channel monitoring.

transmit indicator The indicator on the PMC that blinks red when traffic is being transmitted.

trunk 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.

trunked (system) Systems with full feature sets in which all aspects of radio operation, including RF channel selection and access, are centrally managed.

trunked radio system 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.

U

user 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 or a supported Cisco IP Phone model. Users may have one or more Cisco IPICS roles, such as system administrator, operator or dispatcher.

unicast Specifies point-to-point transmission, or a message sent to a single network destination.

V

VAD 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.

virtual channel 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 Cisco IP Phone 7960 or Cisco IP Phone 7970.

voice interoperability Voice interoperability enables disparate equipment and networks to successfully communicate with each other.

VoIP 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.

volume indicator The volume indicator on the PMC that shows the current volume level on the channel in a graphical format.

volume up/down buttons The buttons on the PMC that let you control the volume level.

VOX 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.

VTG virtual talk group. A VTG can contain any combination of channels, channel groups, users, and user groups. A VTG can also contain other VTGs.

VTG template Before becoming active, a VTG is in an inactive state as a VTG template. The server stores VTG templates so that they can be automatically activated by a policy or manually activated by a dispatcher. Also known as a preconfigured VTG.

W

wavelength The representation of a signal as a plot of amplitude versus time.

wideband channel Channels that occupy more than 20 kHz.

A

B

C

D

E

F

G

I

J

L

M

N

O

P

Q

R

S

T

U

V

W